

Jonge cyberbreinen vroeggesignaleerd

Afstudeerrapport in het kader van de Executive masteropleiding
Riskmanagement PLD Universiteit Twente



Cyberbreinen maken het verschil.

Je bent onwijs goed met computers en de online wereld is jouw wereld. Je voelt je helemaal thuis in Roblox en je kan niet wachten om de computer op te starten. Programmeren in bijvoorbeeld Python vind je ontzettend interessant en je duikt het liefst de code in. Dan heb je wellicht een cyberbrein.



In opdracht van Stichting Cyberbrein.nl
Henk van Ee, studentnummer 1824252, Sneek, april 2025

Voorwoord

Voor u ligt het onderzoeksrapport "Jonge cyberbreinen vroeggesignaleerd!", een studie die zich richt op het vroeg herkennen van jonge cyberbreinen. Een term die geïntroduceerd is door Remco Spithoven nadat ik vertelde met wat voor soort jongeren ik aan het werk was. Met dank!

In een tijdperk waarin digitale dreigingen en cybercriminaliteit aan de orde van de dag zijn, wordt het steeds belangrijker om jonge mensen met een groot talent voor ICT en cybersecurity tijdig te herkennen en te ondersteunen. Dit onderzoek hoopt een bijdrage te leveren aan het vergroten van onze cyberweerbaarheid door het vergroten van de kennis over jonge cyberbreinen en hoe we ze eerder kunnen (h)erkennen.

Het onderzoek is uitgevoerd in opdracht van Stichting Cyberbrein.nl, met als doel inzicht te verkrijgen in de kenmerken en behoeften van jongeren tussen de 10 en 12 jaar die zich onderscheiden door hun digitale vaardigheden. Door een combinatie van literatuuronderzoek en empirische data, verzameld via vragenlijsten met ouders, leerkrachten, ICT-medewerkers en ethische hackers, is geprobeerd een zo compleet mogelijk beeld te schetsen van deze doelgroep en de kenmerken waaraan ze herkend zouden kunnen worden. Inclusief een controlegroep van ouders van “gewone” kinderen.

De resultaten van dit onderzoek bieden hopelijk waardevolle inzichten en aanbevelingen voor beleidsmakers, onderwijsinstellingen en ouders. Door vroegtijdige signalering en gerichte interventies kan voorkomen worden dat deze jongeren het criminele pad op gaan. Daarnaast kan vroegsignalering hen ook stimuleren om hun talenten op een positieve en constructieve manier in te zetten. Dit rapport beoogt dan ook een bijdrage te leveren aan de ontwikkeling van effectieve programma's en initiatieven die jonge cyberbreinen kunnen ondersteunen en begeleiden.

Ik wil graag iedereen bedanken die heeft bijgedragen aan dit onderzoek. In het bijzonder de ouders, leerkrachten, ICT-medewerkers en ethisch hackers die hun tijd en inzichten hebben gedeeld. Jullie bijdragen zijn van onschatbare waarde gebleken voor de totstandkoming van dit rapport.

Daarnaast gaat speciale dank uit naar Sander: dankzij jou heb ik een eerste keer een unieke inkijk gekregen in een cyberbrein en ben je de directe aanleiding geweest voor mijn huidige betrokkenheid bij en inzet voor het aan de goede kant van de streep houden van jonge cyberbreinen.

Ook dank aan Joppe die met eindeloos geduld het redigeren van dit rapport voor zijn rekening wilde nemen en die ik hopelijk ook heb “aangestoken” om zich in te zetten voor de ontwikkeling en begeleiding van jonge cyberbreinen.

Over geduld gesproken: Peter, dank voor je prima begeleiding vanuit de universiteit en inspiratie om door te gaan en dank voor de vele versies die je hebt becommentarieerd. En dank aan Jan-Willem als tweede lezer.

En last but not least Roos, mijn vriendin, steun en toeverlaat en degene die mij heeft gestimuleerd om dit onderzoek (weer) op te pakken en uiteindelijk ook tot een afronding te komen. Ik hoop dat dit onderzoek zal inspireren tot verdere initiatieven en samenwerkingen die bijdragen aan een digitaal weerbare samenleving. En een zinvol leven voor elk jong cyberbrein. Elke ziel telt!

Henk van Ee

Samenvatting

In onze steeds digitalere samenleving groeit het aantal cyberdreigingen, waarbij jong talent in cybersecurity zowel een risico als een kans vormt. Jongeren met een uitzonderlijk talent voor technologie en hacking, aangeduid als jonge "cyberbreinen", kunnen een belangrijke bijdrage leveren aan de cyberweerbaarheid van de maatschappij. Tegelijkertijd ontbreekt structureel beleid om deze jongeren vroegtijdig te (h)erkennen en op ethische wijze te begeleiden. Dit onderzoek richt zich specifiek op kinderen van 10 tot 12 jaar, omdat de bestaande interventies vooral gericht zijn op oudere leeftijdsgroepen, terwijl de betrokkenheid van jongeren bij hackactiviteiten op steeds jongere leeftijd begint.

De hoofdvraag van dit onderzoek luidt: *Hoe zou een set aan praktische kenmerken eruit kunnen om het talent van jonge cyberbreinen al in groep 7/8 van de basisschool te herkennen?* Door middel van literatuuronderzoek en semigestructureerde vragenlijsten onder ouders, ICT-medewerkers, leerkrachten en ethische hackers, is een set praktische gedragskenmerken opgesteld en getest.

De resultaten tonen aan dat ouders het best in staat zijn om de kenmerken te herkennen, waarschijnlijk door hun nauwe betrokkenheid bij het dagelijks gedrag van hun kinderen. Leerkrachten en ICT-medewerkers hebben meer moeite met het signaleren van deze kenmerken, wat deels veroorzaakt zou kunnen worden door een beperkte kennis van het digitale domein en minder intensieve interacties met de jongeren. Volwassen ethical hackers herkennen veel van de voorgestelde kenmerken uit hun eigen jeugd, wat de relevantie van deze kenmerken onderstreept.

Naast bestaande kenmerken, zoals een sterke analytische vaardigheid en nieuwsgierigheid, zijn mogelijk nieuwe indicatoren geïdentificeerd, waaronder autodidactisch leren, out-of-the-box denken en een bovengemiddelde kennis van netwerken en computers. De resultaten uit dit onderzoek benadrukken de noodzaak van gerichte maar gedifferentieerde training voor ouders, docenten en anderen in de opvoedcontext van een jong cyberbrein en de ontwikkeling van structurele programma's om jonge cyberbreinen op ethische wijze te leren begeleiden. Het onderzoek wijst erop dat deze jongeren uitstekende kandidaten lijken te zijn voor ethische hacking-projecten gezien de gesignaleerde kenmerken waaruit een groot rechtvaardigheidsgevoel opvalt en eerlijkheid.

Vervolgonderzoek is nodig om de set kenmerken verder te verfijnen, bijvoorbeeld door middel van meer kwantitatief onderzoek en via interventies zoals een Capture The Flag waarin de gesignaleerde kenmerken getoetst kunnen worden. De urgentie is hoog mede omdat cybercriminelen minder moeite lijken te hebben jonge cyberbreinen te (h)erkennen.

Inhoud

1. Introductie	5
1.1. Cybercriminaliteit groeiend probleem	5
1.2. De preventie en bestrijding van cybercriminelen.....	5
1.3. Potentieel talent kiest op steeds jongere leeftijd voor cybercriminaliteit.....	6
1.4. Het herkennen van cyberbreinen belangrijk	7
1.5. Relevantie en hoofdvraag.....	7
1.6. Belangrijke begrippen.....	8
2. Theoretisch kader.....	9
2.1. Psychologische kenmerken	9
2.1.1. Intelligentie	9
2.1.2. Introversie	10
2.1.3. Autisme	10
2.2. Antisociale persoonlijkheidskenmerken	11
2.3. Sociaaleconomische kenmerken en sociale aspecten.....	11
2.3.1. De rol van de ouders	11
2.3.2. De rol van vrienden en sociale druk.....	12
2.4. De praktische kenmerken waaraan jonge cyberbreinen mogelijk herkend kunnen worden	12
2.5. Deelvragen	14
3. Methode	15
3.1 Ontwerp en aanpak	15
3.1.1. De Likertschaal	15
3.2. Onderzoekspopulatie en selectie.....	15
3.2.1. Ouders van jonge cyberbreinen.....	15
3.2.2. ICT-medewerkers.....	16
3.2.3. Ethische Hackers.....	16
3.2.4. Leerkrachten Groep 7/8	16
3.2.5. Ouders van “gewone” kinderen	17
3.3 Vragenlijsten: opzet en structuur	17
4. Resultaten.....	19
4.1. Algemene resultaten.....	19
4.2. Resultaten per groep	20
4.3. De resultaten vergeleken met de controlegroep	22
4.3.1. Hogere uitkomsten bij controlegroep.....	22
4.3.2. Gematigde verschillen tussen controlegroep en andere groepen	23
4.2.3. Grote verschillen tussen controlegroep en andere groepen.....	23

4.4. Aanvullende kenmerken en suggesties van respondenten	23
4.4.1. Aanvullende kenmerken	23
4.4.2. De aanvullende kenmerken en de controlegroep	24
4.4.3. Suggesties van respondenten voor het helpen van jonge cyberbreinen	24
5. Discussie	27
5.1. Reflectie op de theorie	27
5.2. Reflectie op de methode: betrouwbaarheid en validiteit	28
5.3. Praktische toepasbaarheid van de resultaten	30
5.4. Aanbevelingen voor toekomstig onderzoek.....	30
6. Conclusie.....	32
6.1. Waarneming door verschillende groepen.....	32
6.2. Sociale en cognitieve aspecten.....	32
6.3. Aanvullende kenmerken	33
6.4. Implicaties voor de praktijk en beleid.....	33
Literatuurlijst.....	35
Bijlage 1: AI-statement	38
Bijlage 2a: Vragenlijst Ouders jong cyberbrein.....	39
Bijlage 2b: Vragenlijst Ouders controlegroep	43
Bijlage 3: Vragenlijst medewerker ICT van een school	46
Bijlage 4: Vragenlijst Ethische Hacker	54
Bijlage 5: Vragenlijst Leerkracht.....	59
Bijlage 6: Capture The Flag Junior	68
Bijlage 7: Voorbeeld van games die worden nagebouwd.....	78
Bijlage 8: Flyer Junior Elektro Tactics	79
Bijlage 9: Handleiding met kenmerken vroegsignalering.....	80
Bijlage 10: Profiel in de praktijk en comment teamcaptain Challenge The Cyber.....	87
Bijlage 11: Online ronselen via Discord.....	88

1. Introductie

1.1. Cybercriminaliteit groeiend probleem

In onze samenleving vormt cybercriminaliteit een steeds groter probleem naast de vele voordelen die technologische vooruitgang brengt (Ministerie van Justitie en Veiligheid, 2024). We zien dat het digitale domein toeneemt qua grootte en qua maatschappelijk belang (Kuner et al., 2017). Deze ontwikkeling leidt ook tot ernstige dreigingen voor onze sterk gedigitaliseerde samenleving, omdat de sterk toegenomen digitalisering steeds meer mogelijkheden biedt om cybercriminaliteit te faciliteren waarbij de pakkans laag is en de opbrengsten hoog (Odinot et al., 2018).

Europol noemt cybercrime dan ook expliciet als één van de belangrijkste bedreigingen (Europol & Internet Organised Crime Threat Assessment, 2024) waarbij zowel statelijke actoren een bedreiging vormen via aanvallen op de kritieke infrastructuur als ook cybercriminele organisaties genoemd worden die ransomwareaanvallen plegen.

Daarnaast geeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) aan in het Cybersecuritybeeld Nederland 2021 (2021) dat de “digitale dreiging” zich blijft ontwikkelen terwijl digitale processen het zenuwstelsel vormen van de maatschappij en dat de weerbaarheid nog onvoldoende is. Die dreiging kan bijvoorbeeld bestaan uit ongeautoriseerde inzage in informatie, zoals communicatie binnen de Rijksoverheid door statelijke actoren of de kans op grootschalige uitval.

Ransomware is een ander voorbeeld van een dreiging waarbij bedrijven vaak veel geld betalen om weer bij hun gegevens te kunnen. Bedrijven worden gehackt, wat leidt tot grote financiële schade evenals reputatieschade. De Autoriteit Persoonsgegevens (2024) stelt in een rapportage dat gebrekkige beveiliging maakt dat twee op de drie bedrijven kwetsbaar zijn voor ransomwareaanvallen. In 2023 zijn er 178 ransomwareaanvallen gemeld bij de AP waarbij vermeld wordt dat één aanval vaak meerdere organisaties tegelijk treft en daardoor loopt het totale aantal getroffen organisaties tot in de vele honderden. Persoonlijke gegevens van miljoenen mensen in Nederland werden geraakt aldus de Autoriteit Persoonsgegevens.

Tegelijkertijd lijkt er een groeiend tekort aan cyberspecialisten en dat wordt bevestigd in het Cybersecuritybeeld Nederland 2024 (2024). Hierin wordt het tekort aan cybersecurityspecialisten gesignaleerd in Nederland, wat de digitale weerbaarheid van het land onder druk zet. De schaarste aan cyberspecialisten vormt een bedreiging voor de collectieve cyberweerbaarheid en vraagt om interventies gericht op het vergroten van de vijver van cyberspecialisten (Verbeek, 2019). Zo schetst het UWV dat binnen Defensie er nu al een tekort is aan cyberspecialisten (UWV, 2020).

Ook in het Internet Organised Crime Threat Assessment van Europol (2024) wordt het groeiende tekort aan cybersecurityspecialisten benadrukt. Het rapport wijst op de toenemende vraag naar gekwalificeerde professionals in de sector, wat leidt tot een aanzienlijke kloof tussen vraag en aanbod. Deze discrepantie bemoeilijkt de inspanningen om cybercriminaliteit effectief te bestrijden en de digitale weerbaarheid te versterken. Het rapport roept op tot gerichte investeringen in opleiding en training om deze kloof te dichten en de capaciteit van wetshandavingsinstanties en andere betrokken partijen te vergroten.

1.2. De preventie en bestrijding van cybercriminelen

Cybercriminelen zijn in een aantal categorieën onder te verdelen zoals statelijke actoren, cybercriminelen, hacktivisten en scriptkiddies (Van der Wagen et al., 2019). Statelijke actoren zijn hackers die in dienst zijn van of werken in opdracht van een nationale overheid. Ze richten zich vaak op spionage, sabotage of geopolitieke invloed. Hun aanvallen zijn meestal geavanceerd en goed gefinancierd. Voorbeelden zijn aanvallen op kritieke infrastructuur of het stelen van staatsgeheimen. Cybercriminelen zijn gericht op financieel gewin. Ze gebruiken bijvoorbeeld ransomware, phishing of creditcardfraude om geld te verdienen. Ze opereren vaak in georganiseerde netwerken en zijn zakelijk ingesteld. Bedrijven worden gehackt, wat leidt tot grote financiële schade evenals reputatieschade (Kumar, 2023). De kans dat bedrijven slachtoffer worden van ransomware is inmiddels een op vijf waarbij het gemiddelde schadebedrag op 300.000 Euro wordt geschat (Bescherm je tegen cyberincidenten - Rabobank, z.d.). Hacktivisten voeren cyberaanvallen uit vanuit ideologische of

politieke motieven. Ze willen bijvoorbeeld overheden of bedrijven onder druk zetten of misstanden aan de kaak stellen. Voorbeelden zijn DDoS-aanvallen of het lekken van gevoelige documenten. Scriptkiddies zijn vaak nog onervaren hackers die met weinig technische kennis kant-en-klare tools gebruiken om systemen aan te vallen, vaak voor de lol of om indruk te maken. De aanvallen zijn meestal minder geavanceerd maar kunnen nog steeds impact hebben.

Het Cybersecuritybeeld Nederland 2024 (Ministerie van Justitie en Veiligheid, 2024) benadrukt dat door de groeiende digitale dreigingen van zowel statelijke als criminele actoren, er bredere en intensievere inspanningen nodig zijn om cybercriminaliteit te bestrijden. Hierbij wordt geadviseerd om risico's op digitale incidenten te beheersen via een brede benadering van risicobeheersing. Basismaatregelen blijven belangrijk om een groot aantal cyberaanvallen effectief te blokkeren maar vragen om voldoende cybersecurityspecialisten.

Het bestrijden van cybercriminaliteit vraagt om aanzienlijke investeringen in zowel preventieve als corrigerende maatregelen. Politie en justitie zetten steeds meer technologieën in om de dreiging te beheersen, en organisaties investeren continu in versterkte beveiliging en bewustwording onder medewerkers. Preventieve maatregelen zoals training en publieke bewustwording zijn essentieel, maar vergen ook voortdurende en steeds grotere inzet aldus het hiervoor genoemde Cybersecuritybeeld Nederland 2024.

1.3. Potentieel talent kiest op steeds jongere leeftijd voor cybercriminaliteit

Cybercriminelen worden steeds jonger (Ministerie van Justitie en Veiligheid, 2024). Dankzij vroege toegang tot technologie en de verleiding van spannende, maar onethische uitdagingen, raken jongeren al op jonge leeftijd betrokken bij hacken (Noordegraaf & Weulen Kranenbarg, 2023). Via platforms als Discord worden zij vaak tijdens het gamen benaderd door cybercriminelen (Bijlage 11). Dit begint subtiel, bijvoorbeeld met een verzoek om een onschuldig lijkend scriptje te schrijven – een vorm van scouting.

Talent lijkt dus verloren te gaan omdat jongeren op steeds lagere leeftijd de eerste stappen zetten op het cyber criminele pad (NCSR, 2023). Onderzoek wijst uit dat 1 op de 6 jongeren tussen de 12 en 17 jaar oud wel eens een cyberdelict heeft gepleegd, bewust of onbewust. In de leeftijdsgroep 16-17 jaar is dit zelfs 33 procent. Het gaat hier om delicten als hacking, identiteitsfraude of het downloaden van films zonder te betalen (Derk-Admin, 2019). Recent onderzoek op basis van zelfrapportage laat zien dat in de groep 12-18 jaar 7% zelf aangeeft betrokken geweest te zijn bij cyberdelicten waarbij gedacht kan worden aan inloggen op een account zonder toestemming of dingen op internet kopen zonder te betalen. In deze leeftijdsgroep wordt door 1% zelfs aangegeven dat ze betrokken zijn geweest bij delicten als het uitvoeren van DDoS-aanvallen of het versturen van virussen (Tollenaar et al., 2024).

De beschikbaarheid van kant-en-klare hackingtools werkt als katalysator (Zand et al., 2020). Zo krijgen jongeren steeds eenvoudiger toegang tot middelen als phishingkits en hackingsoftware, wat hun betrokkenheid bij cybercriminaliteit vergroot (Ministerie van Justitie en Veiligheid, 2023). Hierdoor ontstaat een groep jongeren met bovengemiddelde kennis van het cybercriminele circuit, die niet zelden afglijdt naar reguliere criminaliteit, met risico's voor henzelf én de samenleving (Young et al., 2007).

Tegelijkertijd biedt dit talent kansen. Door jong hacktalent te begeleiden richting cybersecurity kunnen ze bijdragen aan digitale weerbaarheid en het tekort aan specialisten helpen verkleinen (Noordegraaf & Weulen Kranenbarg, 2023; Van der Wagen et al., 2019). De uitdaging is hoe deze ombuiging vorm te geven.

Het CCV bracht in kaart welke interventies bestaan rond jeugd en cybercriminaliteit (CCV, 2023). Er blijkt veel aandacht te zijn voor slachtofferschap en daderschap, maar ook diverse 'witte vlekken' in beleid en aanpak. Zo ontbreekt beleid dat ouders actief betreft bij het voorkomen van hackgedrag. Ook zijn er weinig maatregelen voor (opportunistische) daders en slachtoffers, geen technische interventies om hackgedrag vroegtijdig te signaleren, en ontbreken methoden voor vroegherkenning van jong cybertalent. Daarnaast is de effectiviteit van bestaande initiatieven, zoals het event re_B00TCMP, nog niet aangetoond (re_B00TCMP, z.d.). Tijdens dit event maken jongeren kennis met cybersecuritybedrijven, Defensie en Politie om hen te stimuleren de 'goede kant' te kiezen.

1.4. Het herkennen van cyberbreinen belangrijk

Voordat er succesvolle interventies ontwikkeld kunnen worden om een ombuiging richting een carrière aan de goede kant van de streep mogelijk te maken, moeten we eerst de vraag beantwoorden hoe we jonge cyberbreinen vroegtijdig kunnen herkennen. Het lijkt nu namelijk nog een grotendeels onzichtbare groep. Er is ook nog weinig empirisch onderzoek gedaan naar het kunnen herkennen van cyberbreinen. Ten aanzien van herkenning zien we overwegend literatuur over cybercriminelen die al het verkeerde pad zijn ingeslagen maar dat betreft misschien wel een andere doelgroep.

Het is essentieel om te weten hoe jonge cyberbreinen herkend kunnen worden voordat ze cybercrimineel worden zodat ze goed begeleid kunnen worden. Dit onderzoek richt zich dan ook het leren herkennen van jonge cyberbreinen: hoe zou dat vormgegeven kunnen worden? Specifiek richt dit onderzoek zich op het tijdig herkennen van het talent van deze cyberbreinen, en het doen van aanbevelingen betreffende passende interventies, om te voorkomen dat deze jongeren de (cyber)criminaliteit in gaan.

Bij aanvang van dit onderzoek is uitgegaan van een voorlopige definitie van een jong cyberbrein als een kind tussen 8 en de 15 jaar die opvallend vaardig is in zijn of haar omgang met computers, en die al veel complexere taken kan uitvoeren met een computer in vergelijking met leeftijdsgenoten. Ook heeft hij/zij een bovengemiddelde interesse in allerlei vormen van hacking.

1.5. Relevantie en hoofdvraag

Zoals aangegeven in de introductie is er een groot probleem met het cyberweerbaar houden van onze maatschappij en is er een groeiend tekort aan cyberscurityspecialisten in een sterk gedigitaliseerde maatschappij. De intentie van dit onderzoek is om bij te dragen aan deze complexe zaak door te onderzoeken hoe jonge cyberbreinen eerder herkend kunnen worden. De uitkomsten van dit onderzoek kunnen helpen bij het ontwikkelen van interventies die actoren in staat stellen om jongeren te herkennen die zich mogelijk tot hackers ontwikkelen.

Het primaire doel van dit onderzoek is om te onderzoeken hoe het talent van jonge cyberbreinen al op de leeftijd van groep 7/8 basisschool herkend kan worden. Dit betekent dat de focus ligt op de praktische aspecten, en dat de psychologische kenmerken evenals de sociaaleconomische factoren ten dienste staan van de praktische kenmerken waaraan docenten of andere betrokken volwassenen jonge cyberbreinen concreet kunnen herkennen. In samenhang met dit doel heeft dit onderzoek eveneens als doel om een verkenning te doen richting aanbevelingen voor mogelijk passende interventies voor jonge cyberbreinen.

Om te onderzoeken hoe we jonge cyberbreinen kunnen herkennen wordt een set aan praktische gedragskenmerken opgesteld die de omgeving van jonge cyberbreinen kan helpen bij het vroegtijdig herkennen van jonge cyberbreinen. De onderbouwing van deze praktische gedragskenmerken komt voort uit het theoretisch kader.

De centrale onderzoeksvraag is:

Hoe zou een set aan praktische kenmerken eruit kunnen zien om het talent van jonge cyberbreinen al te kunnen herkennen in groep 7/8 van de basisschool?"

1.6. Belangrijke begrippen

In dit onderzoek zijn een aantal termen die steeds wisselend gebruikt worden en eveneens een grote variëteit aan betekenis genieten. In deze sectie wordt daarom kort weergegeven welke termen gehanteerd worden en wat de definitie is:

Jong cyberbrein: een jong cyberbrein is een kind tussen de 8 en de 15 jaar die opvallend vaardig is in zijn of haar omgang met computers, en die al veel complexere taken kan uitvoeren met een computer in vergelijking met leeftijdsgenoten en veel interesse heeft in hacken.

Hacker: een hacker is een persoon die op een malafide manier gebruik maakt van ICT-vaardigheden door op een niet toegestane wijze controle te krijgen over bepaalde digitale systemen met concrete schade tot gevolg.

Ethisch hacker: een ethische hacker is een hacker die zijn/haar skills juist ten goede inzet om de cyberveiligheid van organisaties en personen te verhogen.

Jongvolwassen hacker: een hacker die ouder is dan 16 jaar.

Jonge hacker: een hacker die jonger is dan 16 jaar. Waar een cyberbrein vaardig is in de omgang met computers, heeft een jonge hacker ook daadwerkelijk dingen gedaan in het digitale domein die regels of zelfs wetten breken.

re_B00TCMP: een eendaags event waar jonge kinderen inzicht krijgen in hoe ze hun talent ook ten goede in kunnen zetten.

“Gewone” kinderen: kinderen die niet op voorhand over een cyberbrein lijken te beschikken.

2. Theoretisch kader

Er bestaat veel literatuur waarin uitvoerig onderzoek is verricht over jonge cyberdelinquenten, hun drijfveren en hun kenmerken. Uit onderzoek naar jonge daders blijkt dat deze groep niet bestaat uit een uniforme groep wanneer we het hebben over hun motivaties en kenmerkende factoren die bijdragen aan het plegen van cybercriminaliteit. In plaats daarvan is deze groep juist divers, en bestaat er een grote variatie aan motivaties om crimineel gedrag te vertonen, of om dit juist niet te doen (Loggen et al., 2023; Zand et al., 2020).

In dit onderzoek gebruiken we drie manieren om de analyse van jonge cyberbreinen te duiden. In de eerste plaats hebben jonge cyberbreinen bepaalde psychologische kenmerken, waaraan we hen kunnen herkennen. Ten tweede heeft deze groep vaak een specifieke sociaaleconomische achtergrond. Ten derde zijn er praktische kenmerken waaraan we jonge cyberbreinen kunnen herkennen. Wellicht dat er overlap zit tussen de laatste groep en voornoemde categorieën. Waar dat zo is, zal dat aangegeven worden.

Uit de literatuur blijkt daarnaast dat er op diverse domeinen tegenstrijdigheden zijn wanneer de vraag gesteld wordt hoe jonge cyberbreinen kunnen worden herkend. De belangrijkste oorzaken van deze tegenstrijdigheden zijn de complexiteit van het onderwerp en het gebrek aan betrouwbaar kwantitatief onderzoek dat ook buiten de specifieke context van die studies geldig is. De aard van de complexiteit ligt ten dele in de pluriformiteit van begrippen. Dit betekent dat er geen eenduidige definities zijn om cyberbreinen dan wel hun karaktereigenschappen te definiëren. Deze observatie zorgt voor een situatie waarin er geen eenheid van taal is, wat het bespreken van het onderwerp substantieel bemoeilijkt.¹

Een tweede reden waardoor dit onderwerp zeer complex van aard is heeft te maken met de pluriformiteit van cyberdelicten die jongeren kunnen plegen. Er zijn belangrijke verschillen tussen de typen cyberdelicten die jongeren plegen, hoe ze dit doen, en de context en motieven daarachter. Zo doen sommige jongeren aan hacken louter uit nieuwsgierigheid, terwijl andere jongeren hacken voor financieel gewin. Daarnaast zijn er jongeren die doen aan doxing als reactie op (online) conflicten, wat het openbaar maken is van gevoelige privé gegevens van de slachtoffers. Deze observatie overlapt ten dele met de pluriformiteit aan begrippen en het gebrek aan de eenheid van taal, maar is tegelijkertijd een verdere complicerende factor in het cyberdomein.

Uit de literatuur komen echter wel signalen en kenmerken naar voren waarmee we een persoon met waarschijnlijkheid kunnen identificeren als een cyberbrein, of zelfs als hacker. Daarnaast is de literatuur vrij toegespitst op het analyseren van daderprofielen en het analyseren van sociologische patronen die op cybercriminaliteit kunnen duiden, maar niet op simpele praktische eigenschappen van de jongeren die dergelijke misdaden begaan.

2.1. Psychologische kenmerken

2.1.1. Intelligentie

In de literatuur over cybercriminaliteit zijn er twee denkstromingen over de rol hiervan. Enerzijds zijn er auteurs die het belang van een hoge intelligentie benadrukken, omdat voor het kunnen inbreken in digitale omgevingen zonder toestemming een hoge intelligentie en kennis nodig is van digitale systemen. Hackers, of potentiële hackers, zijn dus per definitie individuen die een degelijke kennis hebben van de mogelijkheden van de digitale systemen waarmee ze hacken (Bossler & Burruss, 2012; (Van der Wagen et al., 2021).

Tegelijkertijd is er literatuur die stelt dat hackers juist een lage intelligentie hebben, omdat ze niet de langetermijngevolgen van hun hackgedrag overzien. Jongeren die daadwerkelijk malafide gedragingen vertonen in het digitale domein hebben niet de zelfreflectie om de consequenties daarvan te doorgronden. Een dergelijke situatie kan dus gekarakteriseerd worden als kortzichtig en laag intelligent (Donner et al., 2014).

¹ Dit methodologische probleem wordt ook veroorzaakt door de complexiteit van het onderwerp, en door de complexiteit van sociale interacties. Meer kwantitatief onderzoek in dit domein zou de literatuur zeker verder helpen, maar tegelijkertijd is dergelijk onderzoek beperkt aan de context waarin het wordt uitgevoerd.

Een nuance in deze schijnbare tegenstelling kan gevonden worden door te kijken naar de methode en intentie van het hacken. In de situatie waarin een individu zelfstandig uitzoekt hoe een systeem werkt, en daar vervolgens malafide dingen mee onderneemt, kan men spreken van een hoog intelligent individu, omdat deze persoon zelfstandig heeft uitgevonden hoe toegang tot dergelijke systemen kan worden verkregen.

In de situatie waarin een individu door leeftijdsgenoten onder druk wordt gezet om te hacken, kan er juist ook sprake zijn van een lage intelligentie. De redenen hiervoor zijn dat dit individu in een dergelijke situatie louter hackt dankzij de hulp van vrienden of leeftijdsgenoten, en dus zelf betrekkelijk weinig kennis van zaken heeft (Zebel et al., 2014; Van der Wagen et al., 2019).

2.1.2. Introversie

De uitkomsten van het onderzoek door Layman et al. (2005) laten zien dat gevorderde bachelorstudenten informatica bepaalde persoonlijkheidsprofielen en leerstijlen hebben die invloed hebben op hun leerervaringen. Veel van deze studenten hebben een voorkeur voor actieve en visuele leerstijlen (Layman et al., 2005). Daarnaast werd opgemerkt dat bepaalde persoonlijkheidskenmerken, zoals introversie of extraversie, van invloed kunnen zijn op de manier waarop studenten problemen aanpakken en samenwerken. Deze inzichten helpen om onderwijsstrategieën af te stemmen op de behoeften van informaticastudenten.

In de literatuur wordt ook gesproken over introversie in relatie tot hacken waarbij introversie kan bijdragen dat iemand minder offline contacten heeft dan online (Van der Wagen et al., 2019). Een verdiepende diagnostiek is echter nodig om te zien of er causaliteit is tussen hackgedrag en introversie.

2.1.3. Autisme

Er heerst een algemeen stereotype dat autistische jongeren vaak betrokken zijn bij hacken, terwijl de academische literatuur een divers en genuanceerd beeld schetst van deze situatie. Sommige studies wijzen op een hoger risico van hackgedrag bij jongeren met autisme, terwijl andere onderzoeken geen significant verband vinden. De onderliggende vraag die dit oproept is of er een direct verband bestaat tussen autisme en hacken, of dat de ogenschijnlijke relatie tussen beide variabelen voortkomt uit secundaire factoren zoals technologische vaardigheden en interesses.

In diverse onderzoeken wordt een positieve relatie tussen autisme en hackgedrag herkend, waarbij voornamelijk de interesse van autistische jongeren in digitale technologie als verklarende factor naar voren komt. Het onderzoek van Payne et al. (2019) laat bijvoorbeeld zien dat een toename van autistische kenmerken samenhangt met een toegenomen kans op hacken. 40% van het verband tussen autistische kenmerken en een toegenomen kans op hacken wordt verklaard door het hebben van digitale vaardigheden, wat impliceert dat de technologische interesse in plaats van het autisme zelf verantwoordelijk is voor het hackgedrag. Lim et al. (2023) ondersteunen deze conclusie door te stellen dat autistische personen vaker structuur en technische uitdagingen opzoeken, waardoor deze personen vatbaarder zijn voor activiteiten zoals hacken. Het onderzoek van Seigfried-Spellar et al. (2015) bevestigt dit beeld wederom, door te benadrukken dat autistische jongeren vaak sterk gefocust zijn en daardoor beter in staat zijn om ingewikkelde digitale systemen te begrijpen in vergelijking tot hun leeftijdsgenoten. De focus en technische bekwaamheid dragen daarmee bij aan een verhoogde kans op hackgedrag. Dit geschetste beeld uit de literatuur laat zien dat de relatie tussen autisme en hackgedrag voornamelijk indirect is, waarbij technologische vaardigheden en persoonlijke interesses een sleutelrol spelen.

Zoals eerder benoemd komt uit andere onderzoeken juist een negatieve correlatie of überhaupt geen correlatie naar voren tussen hackgedrag en autisme. Zo vonden Loggen et al. (2023) geen statistisch significant verband tussen hacken en het hebben van een autismespectrumstoornis, wat de suggestie met zich meebrengt dat autisme geen directe voorspeller is van cybercriminaliteit. Dit sluit gedeeltelijk aan op het onderzoek van Van der Wagen et al. (2021) die een verhoogde kans op autisme bij cyberdelinquenten rapporteerden, zonder de aard van deze relatie verder te duiden. Hun onderzoek benadrukte voornamelijk dat cyberdelinquenten doorgaans introvert zijn, wat een karaktereigenschap is die niet uitsluitend aan autistische jongeren kan worden toegeschreven, waardoor autisme als verklaring minder overtuigend is.

Het verschil tussen de uiteenlopende bevindingen van de academische literatuur over de relatie tussen autisme en hackgedrag kan worden verklaard door de diversiteit aan gebruikte methodologieën en verschillende contexten. Een voorbeeld hiervan zijn de verschillende onderzoekspopulaties die als basis dienden voor het gedane onderzoek. Terwijl het onderzoek van Seigfried-Spellar et al. (2015) zich bijvoorbeeld richtte op ICT-studenten waren er ook onderzoekers die een bredere populatie gebruikten, zoals internetgebruikers in het algemeen (Henderson et al., 2014; Lim et al., 2023; Payne et al., 2019; Wagner et al., 2022). Waar sommige onderzoekers zich richten op specifieke technologische vaardigheden bij autisten, benadert de andere groep het bredere sociale en psychologische profiel van hackers, zonder autisme als bepalende factor te zien. De literatuur laat daarmee dus zien dat de relatie tussen autisme en hacken complex is, en afhangt van meerdere contextuele en methodologische factoren.

2.2. Antisociale persoonlijkheidskenmerken

Op dit moment is het nog niet volledig duidelijk in hoeverre antisociale persoonlijkheidskenmerken zoals impulsiviteit, gebrek aan empathie, en agressiviteit een rol spelen bij cybercriminaliteit. Een gangbare hypothese is dat jonge hackers dergelijke karaktereigenschappen bezitten, waardoor ze niet geremd worden door empathie voor anderen. Tegelijkertijd is er wederom nog geen kwantitatieve studie gedaan die exact meet in hoeverre dergelijke eigenschappen relevant zijn (Kranenbarg et al., 2023; Zebel et al., 2014). Loggen et al. (2023) schrijven bovendien over een negatieve relatie tussen ‘agreeableness’ en hacken, wat het idee dat antisociale persoonlijkheidskenmerken een verklaring is voor hacken versterkt.

2.3. Sociaaleconomische kenmerken en sociale aspecten

Bij de sociaaleconomische factoren is een vergelijkbaar beeld als bij de psychologische factoren, namelijk dat er literatuur is die elkaar tegenspreekt. Daarom geeft deze sectie wederom een beknopt overzicht van de bestaande academische visies over onderwerp en worden de nuances in het debat besproken.

Uit onderzoek is gebleken dat cybercriminaliteit vaak wordt gepleegd door jonge autochtone mannen met een vrij goede sociaaleconomische achtergrond. Bij cybercriminelen die als doel hebben om geld buit te maken ligt de leeftijd waarop ze beginnen met het plegen van misdrijven hoger, en gaat het vaker om allochtone daders, en is er juist sprake van een lagere sociaaleconomische status (Van der Wagen et al., 2019).

2.3.1. De rol van de ouders

Uit onderzoek blijkt dat jongeren die zich schuldig maken aan cybercriminaliteit vaak in een sociaal isolement verkeren in de fysieke wereld, soms veroorzaakt door introversie en autisme. Vanwege dit isolement zoeken deze jongeren naar een vluchtweg in de digitale wereld, waar ze de verbinding en erkenning vinden die ze zoeken (Zand et al., 2020).

Het hebben van een goede band met de ouders wordt vaak gezien als een beschermende factor tegen het plegen van criminaliteit in het algemeen. Dit geldt ook voor cybercriminaliteit (Hirschi, 1969; Zebel et al., 2014). Een stabiele en positieve relatie met ouders kan een remmende werking hebben op het criminele gedrag van jongeren. Toch laat onderzoek ook zien dat bepaalde gezinsstructuren, zoals stiefgezinnen en éénoudergezinnen, vaker samenhangen met hackgedrag onder jongeren (Zebel et al., 2014). Dit kan komen doordat de dynamiek in deze gezinnen anders is, waardoor jongeren mogelijk minder toezicht of begeleiding ervaren.

Daarnaast blijkt dat in gezinnen waar beide ouders fulltime werken, de kans op cybercriminaliteit groter is. Dit komt waarschijnlijk doordat ouders in deze situatie minder tijd hebben om toezicht te houden op hun kinderen. Zonder dit toezicht hebben jongeren meer ruimte om zich in te laten met malafide online-activiteiten.

Hoewel deze factoren een verhoogd risico kunnen vormen, laat de literatuur ook zien dat jongeren uit een goede gezinsachtergrond zich soms toch ontwikkelen tot hackers. Dit geeft aan dat

cybercriminaliteit niet alleen samenhangt met toezicht en gezinsstructuur, maar ook door andere factoren beïnvloed kan worden (Van der Wagen et al., 2019).

Een probleem dat in de literatuur wordt vermeld over de rol van ouders is dat ouders vaak niet begrijpen wat hun kinderen online doen. Dit wijst op een negatief verband tussen digitale kennis bij de ouders en de waarschijnlijkheid dat hun kinderen gaan hacken. Maar tegelijkertijd is het mogelijk dat ouders met technische beroepen, en dus met meer kennis over het digitale domein, een interesse bij hun kinderen aanwakkeren hierover, en juist daardoor zorgen dat hun kinderen gaan hacken (Van der Wagen et al., 2019).

2.3.2. De rol van vrienden en sociale druk

Een andere verklaring voor hackgedrag onder jongeren is de sociale context waarbinnen jongeren zich begeven. Het is voor jongeren belangrijk om het respect te verdienen van hun vrienden, wat hen ertoe kan aanzetten om malafide zaken te doen in het digitale domein, met als doel om respect en aanzien te vergaren. Daarnaast is het online hacken voor jongeren een opwindende ervaring, wat een andere verklaring is voor hun gedrag (Van der Wagen et al., 2021; Loggen et al., 2023).

Tegelijkertijd wordt in de literatuur gezien dat de aanwezigheid van vrienden als oorzaak van hacken minder belangrijk is dan bij regulier crimineel gedrag. Dit betekent waarschijnlijk dat het verband tussen het hebben van vrienden die cyberbreinen hebben, het plegen van hacks en de sociale druk om dat te doen per context verschillend werkt (Van der Wagen et al., 2019).

Er zijn dus diverse redenen waarom jongeren beginnen met hacken. Jonge cyberbreinen worden gemotiveerd door uitdaging, verveling, financiële verrijking, experimenteergedrag of voor de kick die het hacken hen geeft (Bachmann, 2013; Noordegraaf & Weulen Kranenbarg, 2023). Dit gedrag kan vele oorzaken hebben, en kan komen door nieuwsgierigheid, maar kan ook een opstap zijn naar serieuzer crimineel gedrag. Daarnaast voelen jongeren zich vaak vrijer in het digitale domein. Hun handelen wordt minder gecontroleerd, en de consequenties voelen minder echt aan (Zebel et al., 2014).

Externe prikkels zoals sociale status lijken een minder belangrijke rol te spelen in dit proces (Noordegraaf & Weulen Kranenbarg, 2023; Van der Wagen et al., 2019). Het blijkt dat de weg naar (ethisch) hacken vaak ontstaat uit een vroege interesse in ICT, en een verlangen om te weten hoe dingen werken (Bachmann, 2013; Kranenbarg et al., 2022).

De werkelijkheid is complex, waardoor kenmerken vaak overlappen. Stel dat jonge cyberbreinen psychologisch gezien vaak hoog consciëntieus zijn en dat ze als praktisch kenmerk een rijke woordenschat hebben. Dan kun je zeggen dat die uitgebreide woordenschat deels voortkomt uit hun hoge consciëntieusheid, terwijl het in de literatuur als twee aparte kenmerken staat beschreven. Een mogelijke sociaaleconomische factor hierbij is dat hun ouders hoogopgeleid zijn. In de praktijk lopen deze disciplines dus meer in elkaar over dan hier wordt gesuggereerd.

2.4. De praktische kenmerken waaraan jonge cyberbreinen mogelijk herkend kunnen worden

Uit het theoretisch kader komt naar voren dat jongeren met een bovengemiddelde interesse in technologie en ICT specifieke psychologische en gedragsmatige kenmerken vertonen. Deze kenmerken zijn vaak nauw verbonden met zowel hun technische nieuwsgierigheid als hun vermogen om analytisch te denken en creatieve oplossingen te bedenken. Daarnaast wijzen studies op de invloed van hun interacties binnen digitale omgevingen, die hun vaardigheden verder versterken.

Tegelijkertijd laat de literatuur zien dat dergelijke relaties vaak afhankelijk zijn een bepaalde context, en dat de definiëring van begrippen niet consistent is tussen verschillende onderzoeken. Mede hierdoor is het relevant om te onderzoeken in hoeverre de indicatoren uit de literatuur daadwerkelijk praktisch toepasbaar zijn, en in hoeverre bepaalde onderzoeken wellicht niet toepasbaar zijn in de Nederlandse context.

Autisme verdient een aparte vermelding hier: er is bewust gekozen om autisme niet op te nemen in een lijst met praktische kenmerken maar de focus te leggen op feitelijk gedrag dat misschien zijn oorsprong vindt in autisme maar feitelijk herkenbaar moet zijn en vooral ook: kan duiden op een talent. Datzelfde geldt voor andere psychologische factoren zoals introversie.

De theoretische inzichten worden vertaald naar een aantal niet-limitatieve praktische gedragskenmerken die mogelijk indicatief zijn voor een jong cyberbrein en toetsbaar lijken in het vervolg van dit onderzoek:

1. Hebben opvallend veel interesse in en kennis van computers en hoe ze werken

Dit kenmerk van jonge cyberbreinen komt voort uit hun intrinsieke motivatie om technologie te doorgronden. Jongeren met aanleg voor hacken tonen vaak al op jonge leeftijd een sterke interesse in computers, wat wordt gekoppeld aan hun “leerhonger”, intelligentie en experimenteergedrag (Bossler & Burruss, 2012; Payne et al., 2019; Lim et al., 2023; Bachmann, 2013).

2. Hebben opvallend veel kennis van digitale systemen (internet, netwerken)

Veel jonge cyberbreinen leren zichzelf complexe technische concepten aan, zoals netwerken of internetprotocollen. De literatuur noemt dit autodidactisch gedrag en benadrukt dat deze jongeren vaak op eigen initiatief digitale systemen verkennen (Seigfried-Spellar et al., 2015; Van der Wagen et al., 2019; Payne et al., 2019).

3. Zijn zeer nieuwsgierig

Nieuwsgierigheid is een drijvende kracht achter het gedrag van jonge cyberbreinen. Ze zoeken actief naar nieuwe kennis, experimenteren veel, en willen weten hoe dingen werken — een motief dat in meerdere studies naar hackgedrag naar voren komt (Bachmann, 2013; Noordegraaf & Weulen Kranenbarg, 2023).

4. Hebben oog voor detail

Cyberbreinen vallen op doordat ze patronen en fouten opmerken die anderen vaak over het hoofd zien. Deze focus op details is een cognitief kenmerk dat hen helpt bij het analyseren van systemen en oplossen van technische problemen (Seigfried-Spellar et al., 2015; Layman et al., 2005).

5. Hebben een hyperfocus om iets op te lossen en gaan door tot het is opgelost

Hyperfocus of intense concentratie is een belangrijk kenmerk bij deze jongeren, die vaak de tijd vergeten tijdens het oplossen van problemen. Deze gedrevenheid is sterk gerelateerd aan hun motivatie en zorgt ervoor dat ze niet opgeven voordat een technische uitdaging volledig is opgelost, wat kan wijzen op een uitzonderlijk doorzettingsvermogen. Deze hyperfocus wordt in de literatuur regelmatig gelinkt aan autistische trekken, waarbij technische uitdagingen structuur en voldoening bieden (Lim et al., 2023; Seigfried-Spellar et al., 2015).

6. Weten hoe technische dingen werken en helpen de leerkracht daarmee

Veel jonge cyberbreinen laten hun vaardigheden vaak zien door leerkrachten of klasgenoten te helpen met technische problemen. Deze actieve houding komt deels voort uit een thuissituatie waarin digitale interesse wordt gestimuleerd, maar kan ook ontstaan doordat jongeren erkenning vinden via hun vaardigheden (Van der Wagen et al., 2019; Zebel et al., 2014).

7. Halen apparaten uit elkaar halen om te snappen hoe de werking is

Dit gedrag komt voort uit een diepgewortelde nieuwsgierigheid en het verlangen om apparaten letterlijk van binnenuit te begrijpen. Het uit elkaar halen van apparaten komt voort uit een sterke leerdrang en de behoefte om systemen letterlijk van binnenuit te begrijpen. Dit gedrag wordt gezien als een vorm van praktische zelfstudie (Bachmann, 2013; Noordegraaf & Weulen Kranenbarg, 2023).

8. Denken Out of the box

Het vermogen om buiten de gebaande paden te denken, kenmerkt jonge cyberbreinen. Hun creatieve benadering van problemen wordt vaak genoemd als een van de eigenschappen die hen onderscheidt van leeftijdsgenoten. Deze eigenschap stelt hen in staat om onconventionele oplossingen te bedenken voor technische vraagstukken (Van der Wagen et al., 2019; Bachmann, 2013).

9. Een bovengemiddelde beheersing van de Engelse taal

Veel jonge cyberbreinen gebruiken internationale (vaak Engelstalige) online bronnen en forums, wat hun taalbeheersing vergroot. Deze vaardigheid wordt versterkt doordat veel technische documentatie en tools in het Engels beschikbaar zijn (Van der Wagen et al., 2019).

10. Beschikken over sterke analytische vaardigheden

Analytisch denken is een essentieel kenmerk bij het oplossen van complexe technische problemen. De literatuur beschrijft dat jongeren met aanleg voor hacken vaak beschikken over sterke cognitieve vaardigheden waarmee ze systemen kunnen doorgronden (Bossler & Burruss, 2012; Van der Wagen et al., 2021).

11. Hebben veel online contacten en wat minder offline sociale contacten/relaties

Cyberbreinen voelen zich vaak meer thuis in online omgevingen, waar ze gelijkgestemden ontmoeten en hun interesses kunnen delen. Dit gedrag hangt samen met introversie en een zekere mate van sociaal isolement in de offline wereld (Zand et al., 2020; Van der Wagen et al., 2019; Layman et al., 2005).

2.5. Deelvragen

De centrale vraag is opgesplitst in een aantal deelvragen. De **eerste deelvraag** die gesteld wordt is: “In hoeverre herkennen de actoren in de opvoedcontext de set aan praktische kenmerken uit het theoretisch kader?”. Op basis van deze deelvraag wordt gecheckt bij relevante actoren die in hun werk of dagelijks leven te maken hebben met cyberbreinen of ze inderdaad jonge cyberbreinen uit hun eigen praktijkervaring kunnen herkennen. De relevante actoren zijn docenten, medewerkers ICT, ouders van jonge cyberbreinen, en ethische hackers. Als controlegroep hebben we ouders van “normale” kinderen gebruikt. Dit gebeurt aan de hand van de lijst praktische kenmerken vanuit het theoretisch kader. De actoren hier zijn ouders en medewerkers ICT van een basisschool/onderbouw Voortgezet Onderwijs.

De **tweede deelvraag** die we stellen is “In hoeverre herkennen (jong)volwassen ethische hacker zich in de set aan praktische kenmerken van een jong cyberbrein?”

Op basis van deze deelvraag willen we bij deze ervaringsdeskundigen checken of de set aan praktijk indicatoren correct is of ze zich dus herkennen en ook zouden herkennen toen ze zelf op de lagere school zaten.

Een aanvullende **derde deelvraag** is: "Welke kenmerken ontbreken mogelijk nog?".

Het is immers goed denkbaar dat het bestaande onderzoek nog niet volledig is, en dat er meer patronen, kenmerken, gedragsindicatoren of fenomenen zijn waaraan we cyberbreinen kunnen herkennen. Daarnaast is het zo dat mensen uit het werkveld en ouders mogelijk specialistische kennis meebrengen die nog niet in de literatuurverkenning naar voren is gekomen.

De bestaande literatuur evenals empirische gegevens spitsen zich uitsluitend toe op middelbare scholieren en jongeren die nog ouder zijn. Er is dus nog weinig onderzoek gedaan naar de groep jonge cyberbreinen van 12 jaar en jonger. Om die reden focust dit onderzoek zich hoofdzakelijk op jongeren die in groep 7 of 8 van de basisschool zitten.

Hierbij zijn twee aannames van belang. Allereerst nemen we voor dit onderzoek aan dat het mogelijk is om jonge cyberbreinen te herkennen wanneer deze nog in groep 7 of 8 van de basisschool zitten. Daarnaast nemen we aan dat het zinvol is om deze jongeren zo vroeg mogelijk te signaleren, met het idee dat we hun talenten dan kunnen benutten, en met het idee dat ze zo op het rechte pad blijven. Daar is ook wel aanleiding voor omdat deze jongeren al op deze leeftijd in aanraking kunnen komen met (cyber)criminelen die jongeren met ICT-skills ronselen.

In deze deelvraag wordt ter controle ook onderzocht in hoeverre ouders van jongeren die niet op voorhand als cyberbrein te categoriseren zijn, de kenmerken herkennen bij hun kinderen.

De **vierde deelvraag** die gesteld wordt, is: “in hoeverre herkennen leerkrachten van groep 7/8 aan de hand van de mogelijk bijgewerkte set aan gedragskenmerken jonge cyberbreinen onder hun leerlingen?” Met deze deelvraag wordt gekeken of de set aan gedragskenmerken in de praktijk ook werkt.

De **vijfde deelvraag** die we stellen is “Wat zouden jonge cyberbreinen in groep 7/8 nodig hebben om hun talenten te ontwikkelen?”

Met deze deelvraag wil de onderzoeker een aanzet doen voor interventies voor deze specifieke doelgroep. Deze vraag zal aan de (jong-) volwassen ethische hackers en aan ouders van jonge cyberbreinen gesteld worden.

3. Methode

Dit hoofdstuk bespreekt de methodologie die is gehanteerd om de onderzoeksvraag te beantwoorden en biedt inzicht in de onderzoeksopzet, de steekproefselectie, de data-verzamelingstechnieken, en de overwegingen die hebben geleid tot deze keuzes. Het primaire doel van dit onderzoek was om een set aan praktische gedragskenmerken te valideren die gebruikt kunnen worden voor het identificeren van jonge cyberbreinen in de basisschoolleeftijd, met name groep 7 en 8. Hiertoe zijn online vragenlijsten en aanvullend literatuuronderzoek ingezet om inzicht te verkrijgen vanuit de percepties van ouders, leerkrachten, ICT-medewerkers, en volwassen ethische hackers.

3.1 Ontwerp en aanpak

In dit onderzoek is gekozen voor een exploratief onderzoeksontwerp met een focus op semigestructureerde vragenlijsten. Dit type vragenlijst combineert zowel gestructureerde vragen als open vragen, zodat respondenten ruimte hebben om hun antwoorden te onderbouwen of extra toelichting te geven. Deze flexibiliteit is essentieel om het domein van het onderzoek, dat nog relatief nieuw en onderbelicht is, volledig te kunnen exploreren. Door het gebruik van semigestructureerde vragenlijsten wordt zowel een zekere mate van consistentie in de antwoorden gewaarborgd als de mogelijkheid om unieke, onvoorziene inzichten te verzamelen.

De vragenlijsten zijn gericht op het identificeren van de praktische gedragskenmerken die kunnen wijzen op het hebben van een cyberbrein. Hierbij is bijzondere aandacht besteed aan de perceptie van verschillende groepen betrokkenen, namelijk ouders, ICT-medewerkers, leerkrachten en volwassen ethische hackers. Het perspectief van deze verschillende groepen biedt een breed beeld en maakt het mogelijk om de relevantie van de geïdentificeerde gedragskenmerken te toetsen in diverse contexten. Het exploratieve karakter van dit onderzoek maakte dat aanvullende kenmerken eveneens konden worden verzameld, naast de kenmerken die in de literatuur zijn geïdentificeerd en praktisch zijn gemaakt.

3.1.1. De Likertschaal

Voor dit onderzoek is gebruik gemaakt van de Likertschaal, waarbij respondenten vijf antwoordopties kregen om gesloten vragen te beantwoorden. Deze vragen richtten zich op de mate waarin zij praktische gedragskenmerken herkenden bij jonge cyberbreinen in hun omgeving. Alle groepen konden antwoorden tussen 1 en 5 geven, met uitzondering van de docenten, die ook de optie 0 kregen. Dit verschil in antwoordopties is onbedoeld ontstaan en vormt een methodologische beperking van het onderzoek, omdat docenten een andere antwoordmogelijkheid hadden die bij de andere groepen niet beschikbaar was. Hierdoor kunnen de gemiddelde scores van de docenten lager uitvallen dan die van andere groepen, omdat zij een extra lage antwoordmogelijkheid hadden. Bij de interpretatie van de resultaten moet hiermee rekening worden gehouden om eerlijke vergelijkingen te kunnen maken.

3.2. Onderzoekspopulatie en selectie

In dit onderzoek zijn vijf groepen respondenten benaderd om data te verzamelen: ouders van jonge cyberbreinen, ICT-medewerkers van basisscholen, volwassen ethische hackers en leerkrachten van groep 7/8. Elk van deze groepen heeft een unieke relatie met de beoogde doelgroep van het onderzoek, namelijk jongeren met potentieel cyberbrein, en draagt bij aan een bredere validatie van de kenmerken. Ter controle is er ook een vragenlijst voorgelegd aan ouders van “gewone” kinderen en die dus niet lijken te voldoen aan het profiel van een jong cyberbrein.

3.2.1. Ouders van jonge cyberbreinen

De keuze om ouders bij het onderzoek te betrekken is gebaseerd op hun dagelijkse interactie met hun kinderen, waardoor zij vaak een goed beeld hebben van het gedrag en de talenten van hun kind. Voor de ouders is een vragenlijst opgesteld waarin zij gevraagd werden naar de mate waarin zij bepaalde

gedragskenmerken bij hun kind herkennen. Deze kenmerken zijn opgesteld op basis van het theoretisch kader en omvatten bijvoorbeeld nieuwsgierigheid naar technologie, een neiging om apparaten te ontleden en een voorkeur voor technische puzzels.

In totaal hebben 16 ouders deelgenomen aan de vragenlijst. De selectie van deze ouders vond plaats via directe contacten met gezinnen waarvan kinderen deelnamen aan activiteiten zoals de re_B00TCMP, een evenement waar jonge hacktalenten door middel van een assessment worden getest op hun ICT-vaardigheden. Deze benadering zorgt ervoor dat de ouders in de steekproef relevante ervaringen hebben met kinderen die over bovengemiddelde digitale vaardigheden beschikken. Het aantal respondenten is echter beperkt, wat een mogelijk risico vormt voor de generaliseerbaarheid van de resultaten.

3.2.2. ICT-medewerkers

ICT-medewerkers binnen het onderwijs hebben een andere kijk op de digitale vaardigheden van leerlingen. Door hun kennis van technologie kunnen zij gedrag herkennen dat mogelijk wijst op het hebben van een cyberbrein. De vragenlijst voor deze groep was gericht op de observatie van gedrag op school en de interactie van leerlingen met technologie. Zij werden gevraagd naar herkenbare gedragskenmerken zoals nieuwsgierigheid naar technologie en nieuwsgierigheid.

In totaal hebben 14 ICT-medewerkers de vragenlijst ingevuld. De selectie van deze groep vond plaats via persoonlijke netwerken, waaronder LinkedIn en via ouders van jonge cyberbreinen die deelnamen aan de vragenlijst. Hoewel deze methode niet volledig aselekt was, bood het een praktisch haalbare manier om respondenten te bereiken die in hun werk regelmatig in aanraking komen met digitale vaardigheden van leerlingen.

3.2.3. Ethische Hackers

Een derde groep die betrokken werd bij dit onderzoek zijn volwassen ethische hackers, personen met praktische ervaring en een diepgaand inzicht in de wereld van cybersecurity. Deze groep bood waardevolle feedback, omdat zij vanuit eigen ervaring kunnen reflecteren op de kenmerken die mogelijk wijzen op talent voor cybersecurity oftewel het hebben van een cyberbrein. Het doel van de vragenlijst voor ethische hackers was om inzicht te krijgen in hun perceptie van de kenmerken die mogelijk ook op jonge leeftijd al zichtbaar waren, en om na te gaan of zij zichzelf herkennen in de geïdentificeerde gedragskenmerken.

In totaal hebben 45 ethische hackers de vragenlijst ingevuld. Deze deelnemers werden geselecteerd via een mix van netwerken, waaronder de DIVD Academy, een netwerk voor ethische hackers, en online gemeenschappen zoals de Discordserver van de re_B00TCMP en het persoonlijke netwerk van de onderzoeker, onder andere via LinkedIn. De relatief hoge respons in deze groep maakt hun input een belangrijke en betrouwbare bron voor de validatie van de gedragskenmerken. Dit brede bereik aan respondenten binnen deze groep verhoogt bovendien de diversiteit en dus de representativiteit van de resultaten.

3.2.4. Leerkrachten Groep 7/8

De leerkrachten van groep 7 en 8 zijn belangrijke actoren in de vroegsignalering van jonge cyberbreinen. Voor deze groep werd een aangepaste vragenlijst opgesteld die gericht was op het herkennen van gedragskenmerken binnen de schoolomgeving. Vanwege hun positie in de onderwijsketen kunnen leerkrachten observeren hoe leerlingen reageren op technische en analytische uitdagingen. Het doel was om vast te stellen of de geïdentificeerde kenmerken daadwerkelijk behulpzaam zijn voor deze doelgroep in het herkennen van cyberbreinen.

Door tijdsbeperkingen en moeilijkheden in de onderzoeksperiode konden slechts zeven leerkrachten de vragenlijst invullen. Dit beperkte aantal deelnemers is een risico voor de betrouwbaarheid en representativiteit van de bevindingen. Bovendien was er oorspronkelijk gepland om de geselecteerde leerlingen die door leerkrachten als potentieel cybertalent waren herkend, te laten deelnemen aan een digitale Capture the Flag-test (Bijlage 6), maar deze toetsing bleek binnen de onderzoeksperiode niet uitvoerbaar.

3.2.5. Ouders van “gewone” kinderen

Het profiel van een jong cyberbrein is inclusief de aanvullende kenmerken door ethische hackers, in een online vragenlijst (Bijlage 2b) voorgelegd aan ouders van “gewone” kinderen. Kinderen dus die waarschijnlijk niet over een cyberbrein beschikken. Dit betreft dus een controlegroep om selectiebias te voorkomen. De selectie van deze groep heeft plaatsgevonden door ouders uit het persoonlijke netwerk van de onderzoeker te benaderen. Er zijn 21 ouders die de vragenlijst hebben ingevuld.

3.3 Vragenlijsten: opzet en structuur

De vragenlijsten in dit onderzoek zijn semigestructureerd opgesteld en bevatten een combinatie van gesloten en open vragen. Deze aanpak stelt respondenten in staat om niet alleen keuzes te maken, maar ook hun ervaringen en observaties in eigen woorden te delen. Per groep respondenten hebben we een verschillende vragenlijst met elk aparte vragen.

We hebben de praktische kenmerken die uit de literatuur komen voorgelegd aan de verschillende groepen van respondenten, waarbij ze konden aangeven in hoeverre de praktische kenmerken wel of geen betrekking hadden op hun persoonlijke situatie. Voorbeelden van deze praktische kenmerken zijn zaken als Engels taalbeheersing, analytische vaardigheden, en apparaten uit elkaar halen om te zien hoe deze werken. Vervolgens kregen de respondenten de mogelijkheid om bij een open vraag aanvullende informatie te geven over de motivaties achter hun antwoorden.

Aanvankelijk hebben we met 11 praktische kenmerken gewerkt. Omdat de respondenten zelf met aanvullende kenmerken kwamen, hebben we bij de controlegroep van ons onderzoek deze aanvullende kenmerken meegenomen, en hebben we de ouders van normale kinderen in totaal hun mening laten geven over 16 kenmerken. Dit hebben we gedaan om in kaart te brengen of de aanvullende kenmerken daadwerkelijk van toepassing zijn op jonge cyberbreinen, of dat dit verschijnselen zijn die ook bij normale kinderen zichtbaar zijn. Daarnaast hebben we bij docenten ook de aanvullende kenmerken getoetst.

Zoals eerder vermeld hebben we bij docenten een andere meetmethode (schaalindeling) gebruikt dan bij de andere groepen. Hierdoor is het moeilijk om de resultaten van de docenten één op één met de andere groepen te vergelijken. We hebben ervoor gekozen om de resultaten van de docenten desondanks deze methodologische discrepantie wel samen te voegen bij de andere resultaten, maar het is goed dat de lezer zich hiervan bewust is.

Hier volgen twee voorbeelden van vragen met open antwoordmogelijkheden bij de verschillende groepen respondenten:

- Herkenning van specifieke gedragskenmerken en aanvullende kenmerken
 - Vraag voor leerkrachten: "In hoeverre kloppen de kenmerken met het beeld dat u heeft van een jong cyberbrein? Zijn er kenmerken die niet genoemd worden, maar die volgens u wel belangrijk zijn?" (Bijlage 5).
 - Vraag voor ouders: "Mist u in de vorige vraag nog (gedrags-)kenmerken of specifieke eigenschappen die u opvallend vindt voor een jong cyberbrein en waar het talent nog meer aan herkend zou kunnen worden?" (Bijlage 2a).
- Relevantie en volledigheid van kenmerken
 - Vraag voor ICT-medewerkers: "Mist u kenmerken die volgens u belangrijk zijn voor het identificeren van jonge cyberbreinen, gebaseerd op uw ervaring op school?" (Bijlage 3).
 - Vraag voor ethische hackers: "Herken jij je als ethische hacker in deze kenmerken die voor een jong cyberbrein zijn opgesteld? Welke typische eigenschappen mis je of zijn nodig om deze set compleet te maken?" (Bijlage 4).

Contextuele factoren

- Vraag voor ouders: "Terugkijkend op de lagere schoolperiode van uw zoon/dochter: wat zou hij/zij aan extra begeleiding/uitdaging/informatie nodig hebben gehad?" (Bijlage 2a).
- Vraag voor leerkrachten: "In hoeverre denkt u dat specifieke kenmerken van cyberbreinen beter tot uiting komen in bepaalde contexten, bijvoorbeeld bij vakken of activiteiten op school?" (Bijlage 5).

- Behoeftte aan ondersteuning en begeleiding
 - Vraag voor ethische hackers: "Wat zou jij nodig hebben gehad op de basisschoolleeftijd om je cybervaardigheden verder te ontwikkelen of meer ondersteuning te krijgen?" (Bijlage 4).
 - Vraag voor ICT-medewerkers: "Wat zou u nodig hebben om een jong cyberbrein goed te kunnen begeleiden binnen de schoolomgeving?" (Bijlage 3).

We hebben de data uit de open vragen verwerkt door alle antwoorden te lezen en vervolgens een samenvatting te geven vanuit deze antwoorden. Hierbij heeft er bij een aantal vragen ook een thematische clustering plaatsgevonden. In elk geval zijn alleen vergelijkbare antwoorden en citaten opgenomen die door minimaal drie respondenten gegeven zijn. Wanneer er interessante antwoorden werden gegeven zijn die soms uitgelicht ter illustratie, of omdat ze een interessant inkijkje gaven over de manier van denken van de respondenten.

Een voorbeeld van thematische clustering is hieronder weergegeven uit vragen die gericht waren op de ouders van jonge cyberbreinen. Deze vragen hadden betrekking op suggesties wat een kind nodig zou hebben op de basisschool. Uit de antwoorden zijn de volgende clusters gehaald: meer mogelijkheden van begeleiding bieden met voldoende technische bagage, meer ICT-uitdagingen bieden, meer kennis over vroegsignaleren in het onderwijs brengen, vertrouwen geven en durven loslaten en bespreken van grenzen.

De volledige vragenlijsten zijn als bijlagen opgenomen bij dit onderzoek.

4. Resultaten

In dit onderzoek hebben we gekeken naar de herkenning van kenmerken van jonge cyberbreinen door diverse betrokken partijen. De betrokken partijen die we hebben onderzocht zijn ouders, ICT-medewerkers, volwassen ethische hackers en leerkrachten. Daarnaast hebben we als controlegroep ouders van reguliere kinderen gevraagd in hoeverre zij de lijst aan praktische kenmerken herkennen bij hun kinderen.

In deze sectie van het onderzoek bespreken we eerst integraal de resultaten en de implicaties die onze resultaten met zich meebrengen. Hierna bespreken we de resultaten apart per groep. We hanteren deze structuur omdat we op die manier eerst bespreken welke variabelen het belangrijkste zijn voor het vroeg signaleren van jonge cyberbreinen (het primaire doel van ons onderzoek), maar tegelijkertijd ook ruimte laten voor aanvullende overwegingen en nuances die meespelen bij de interpretatie van onze resultaten. We eindigen deze sectie met een aantal kwalitatieve uitspraken die de deelnemers van ons onderzoek hebben gedaan die wij relevant achten om te vermelden.

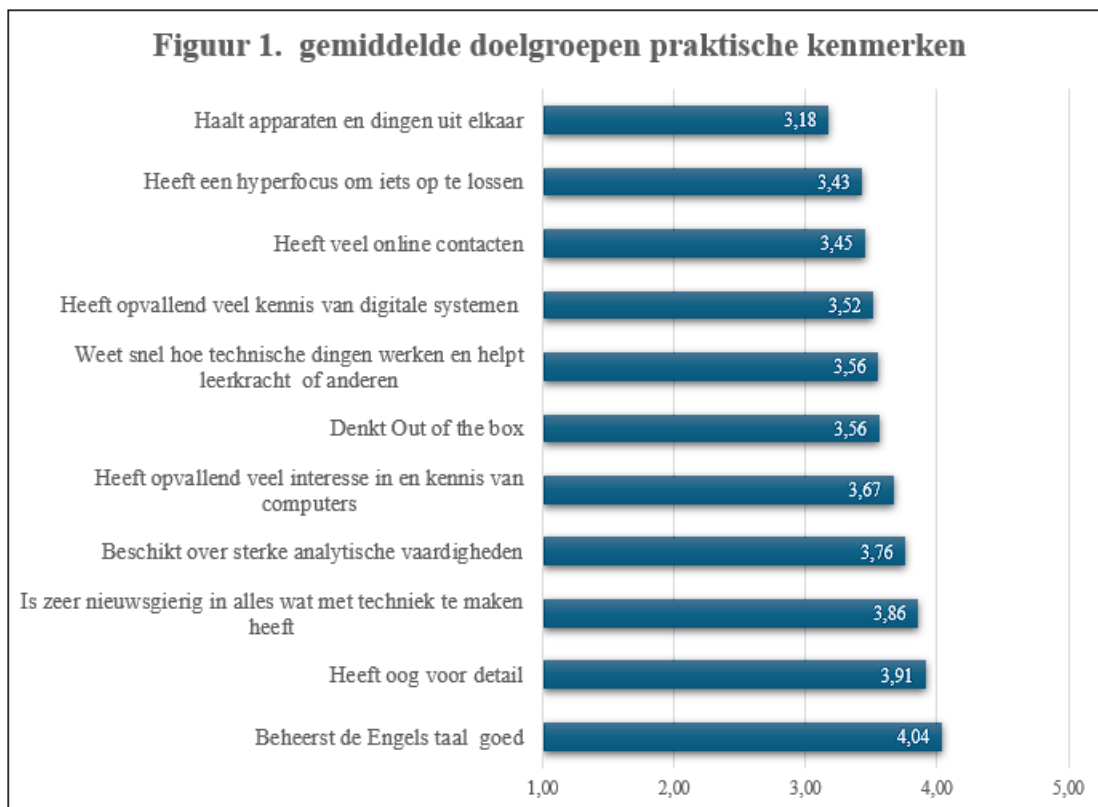
4.1. Algemene resultaten

Uit het onderzoek lijkt dat Engelse taalbeheersing, het hebben van oog voor detail en nieuwsgierigheid de drie belangrijkste kenmerken zijn om jonge cyberbreinen vroegtijdig te herkennen. Deze drie kenmerken hebben namelijk gemiddeld gezien bij alle groepen de hoogste score behaald.

Daarnaast blijkt uit ons onderzoek dat het hebben van veel online contacten, het hebben van een hyperfocus, en het uit elkaar halen van apparaten minder belangrijkere factoren lijken om jonge cyberbreinen aan te herkennen.

Figuur 1 toont een overzicht van alle variabelen en de mate waarin deze variabelen herkend werden door onze respondenten. Het minimale getal wat respondenten konden invullen was een '1', en het maximale getal was een '5'. Het gewogen gemiddelde wat te zien is, is de som van alle respondenten over alle groepen. We hebben 12 ouders, 35 ethische hackers, 7 medewerkers ICT, en 4 leerkrachten geïnterviewd voor dit onderzoek. Dat betekent dat de resultaten van de ethische hackers en de ouders relatief zwaarder meewegen omdat we daar simpelweg meer input van hebben verzameld in verhouding tot de leerkrachten en de medewerkers ICT.

Daarnaast is het soms het geval dat respondenten ervoor kozen om vragen niet in te vullen. Bij de ouders hebben 3 ouders ervoor gekozen om sommige vragen niet in te vullen. Bij de ethische hackers was er 1 hacker die niet alle vragen heeft ingevuld. Bij de medewerkers ICT waren er 3 medewerkers die niet alle vragen hebben beantwoord, en bij de leerkrachten was er 1 leerkracht die niet alle vragen wilde beantwoorden. Hoewel deze factoren afbreuk doen aan de betrouwbaarheid van ons onderzoek, zijn de resultaten afdoende voor het primaire doel van ons onderzoek, omdat we voornamelijk geïnteresseerd zijn in het schetsen van een algemeen beeld over de praktische kenmerken waaraan jonge cyberbreinen herkend kunnen worden. Daarnaast worden de resultaten per groep, zoals eerder al benoemd, nog apart besproken.



Er zijn een aantal zaken die opvallen aan de resultaten die te zien zijn in figuur 1. Om te beginnen is het zo dat alle variabelen hoger scoren dan een 3, wat betekent dat de variabelen allemaal in zekere mate gebruikt kunnen worden om jonge cyberbreinen te herkennen. Te zien is dat Engelse taalbeheersing, het hebben van oog voor detail, en nieuwsgierigheid in techniek het hoogste scoren, terwijl online contacten, het hebben van een hyperfocus en het uit elkaar halen van apparaten het laagste scoren. Daarnaast is het goed om te beseffen dat docenten de optie hadden om 0 in te vullen, terwijl de laagste waarde in deze figuur 1 is.

Wij zijn als onderzoekers in de veronderstelling dat er een positieve relatie bestaat tussen de verbinding die een groep heeft met jonge cyberbreinen, en de mate waarin een dergelijke groep in staat is om de praktische kenmerken uit de literatuur daadwerkelijk te observeren in het gedrag van jonge cyberbreinen. Deze veronderstelling maakt het aannemelijk dat er een discrepantie bestaat tussen de gemeten effectiviteit van de praktische kenmerken en de daadwerkelijke effectiviteit van de praktische kenmerken. Omdat we voornamelijk volwassen ethische hackers hebben geïnterviewd en maar ten dele groepen die op afstand staan van jonge cyberbreinen (docenten en medewerkers ICT) is dit effect beperkt gebleven. In het volgende onderdeel van het onderzoek kijken we mede daarom ook naar de resultaten per groep. We doen dit ten dele om inzichtelijk te krijgen hoe groot de impact is van de specifieke groep waar iemand een onderdeel vanuit maakt, en omdat het ons aanvullende informatie geeft over de bruikbaarheid van de praktische kenmerken.

4.2. Resultaten per groep

Zoals we boven benoemd hebben geeft figuur 1 slechts een beperkt beeld van de werkelijkheid, omdat deze figuur geen rekening houdt met de verschillen per groep en de consequenties hiervan voor het onderzoek. In dit gedeelte van het onderzoek gaan we daarom per groep specifiek een analyse geven van de resultaten.

Bij **ouders** van jonge hackers zijn zestien vragenlijsten afgenomen die betrekking hebben op kenmerken van jonge cyberbreinen, zoals beschreven in de literatuur. De resultaten wijzen op een over het algemeen op een goede herkenning van deze kenmerken door de ouders. Gedragskenmerken zoals oog voor detail (gemiddelde score van 4.36/5), het helpen van de leerkracht 4.00/5) en out of the box

denken (4.20/5) werden bijzonder hoog gewaardeerd. Kenmerken die meer abstract of technisch zijn, zoals sterke analytische vaardigheden en hyperfocus, werden minder vaak herkend (alle scores onder 4.00/5).

Bij **ICT-medewerkers**, waarvan er veertien respondenten deelnamen aan de vragenlijst, was de herkenning van kenmerken veel lager in vergelijking met ouders. De hoogste score was voor kennis van digitale systemen (3.29/5), terwijl eigenschappen zoals out of the box denken (2.75/5) en apparaten uit elkaar halen (2.25/5) veel minder herkend werden.

Bij de volwassen **ethische hackers** is nagegaan of de set praktijkindicatoren klopt. Er is gevraagd of zij zich in deze kenmerken herkennen en of ze deze ook zouden hebben herkend toen ze zelf op de lagere school zaten. De 45 volwassen ethische hackers die de vragenlijst ingevuld hebben identificeerden zich sterk met de kenmerken van jonge cyberbreinen zoals beschreven in de literatuur. Ze gaven hoge scores voor interesse in computers (4.10/5), hyperfocus (4.09/5) en oog voor detail (4.09/5). Dit resultaat lijkt te betekenen dat volwassen hackers goed zijn in het herkennen van de talenten van jonge cyberbreinen, omdat ze zelf vergelijkbare kenmerken hebben.

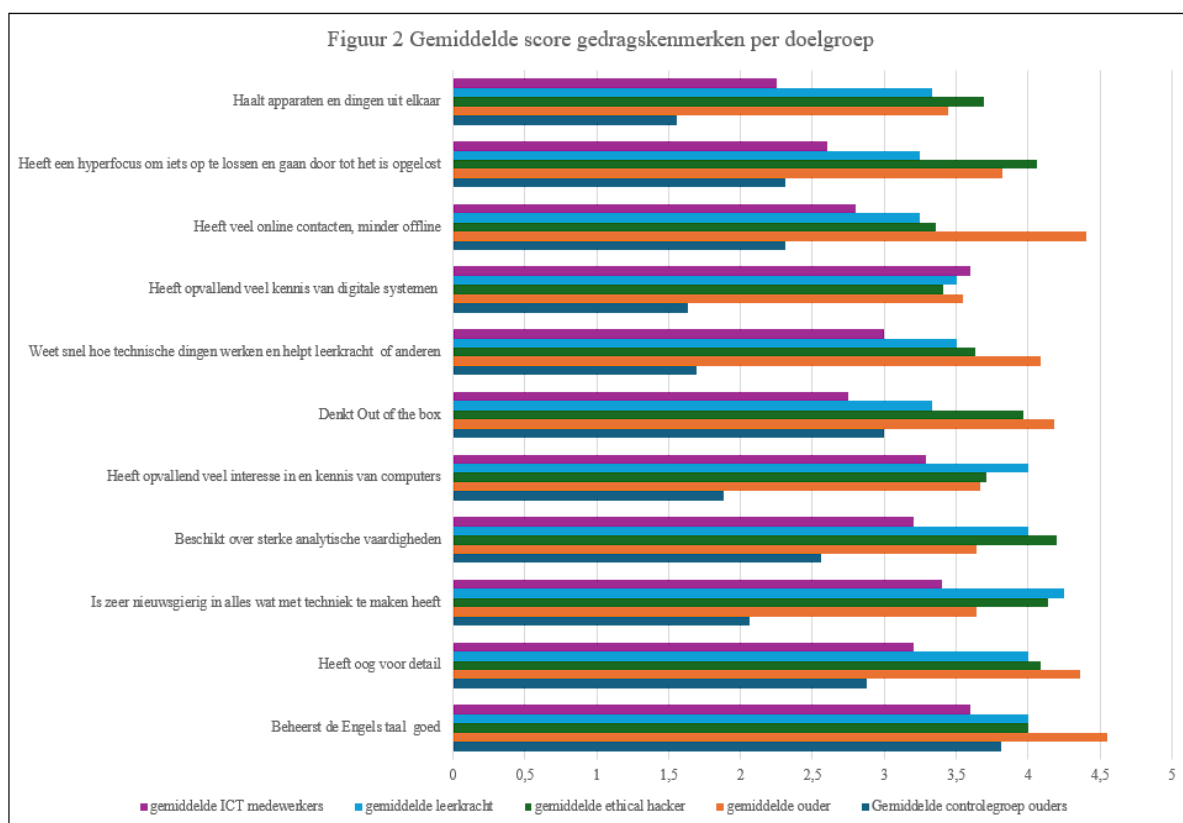
Echter, een complicerende factor die naar voren kwam, was de noodzaak voor een ‘vertaling’ van technologieën van vroeger naar nu. Veel volwassen hackers gaven aan dat ze het belangrijk vonden om duidelijk te maken hoe technologie in de loop der jaren is veranderd en dat dit begrip essentieel is voor het herkennen en ondersteunen van jonge cyberbreinen.

Voor dit onderzoek hebben we ook bij zeven **docenten** een vragenlijst afgenomen. Deze docenten van groep 7/8 gaven aan dat zij een gemiddelde zelfinschatting van hun ICT-kennis hebben van 5.83/10, wat aangeeft dat zij zich bewust zijn van hun beperkingen op dit gebied. Hun lage affiniteit met de digitale wereld van jongeren is een belangrijke constatering en kan reden tot zorg zijn, aangezien zij een cruciale rol spelen in de ontwikkeling en begeleiding van deze kinderen. Dit kan resulteren in het niet volledig herkennen van de unieke talenten en behoeften van jonge cyberbreinen. De leerkrachten leken vooral “hyperfocus op het oplossen van problemen” en “affiniteit met technische en digitale systemen” te herkennen, maar hun beperkte zicht op de digitale wereld van jongeren kan hen beletten om een breder beeld van deze talenten te krijgen.

Slechts drie docenten hebben antwoord gegeven op de aanvullende gedragskenmerken die voortkwamen uit de vragenlijsten met ouders en ethische hackers. Nieuwsgierigheid voor techniek was het kenmerk dat er bij deze groep uitsprong, met een 4.25/5. Bij de andere kenmerken is te zien dat interesse in computers (4.0/5), Engelse taalbeheersing (4.0/5), het hebben van sterke analytische vaardigheden (4.0/5) en het hebben van oog voor detail (4.0/5) hoog scores. Zoals we eerder al benoemden kregen docenten onbedoeld de optie om 0 in te vullen in plaats van 1 als laagste antwoord. Hierdoor zijn de uitkomsten bij docenten waarschijnlijk lager dan bij de andere groepen.

4.3. De resultaten vergeleken met de controlegroep

Wanneer we kijken naar de resultaten per groep in vergelijking tot de controlegroep vallen een paar dingen op (n=24). We zijn hierbij specifiek geïnteresseerd in het vinden van een verschil tussen de controlegroep en de andere doelgroepen uit ons onderzoek, omdat dit ons een situatie verschaft waarin we de gebruikte variabelen daadwerkelijk kunnen gebruiken om jonge cyberbreinen te vroeg signaleren. Kijkende naar de resultaten tussen de controlegroep en de andere groepen vallen een aantal algemene dingen op die we straks per punt bespreken. Hieronder in figuur 2 zijn de resultaten te zien die hieronder worden geanalyseerd en besproken.



Om te beginnen is er bij alle variabelen maximaal één groep geweest die aangeeft dat jonge cyberbreinen **lager** scoren dan reguliere kinderen, namelijk de medewerker ICT. Daarnaast laten de resultaten een schifting zien tussen een aantal variabelen. Specifiek zien we dat er bij sommige variabelen een grote discrepantie is tussen de controlegroep en de andere groepen, terwijl dit verschil bij andere variabelen marginaal is.

4.3.1. Hogere uitkomsten bij controlegroep

Ten eerste valt het op dat er variabelen zijn die bij de controlegroep hoger zijn uitgevallen dan bij sommige groepen van het aanvankelijke onderzoek. Deze variabelen zijn Engelse taalbeheersing en out of the box denken. Deze resultaten impliceren dat deze variabelen geen voorspellende werking geven voor het vroegsignaleren van jonge cyberbreinen, omdat ‘normale’ kinderen deze eigenschappen net zoveel of volgens sommige doelgroepen zelfs meer hebben in vergelijking met jonge cyberbreinen.

Een nuancering van bovenstaand punt is dat het alleen de medewerkers ICT zijn die de betreffende factoren als ‘laag’ hebben ingevuld. Daarnaast weten we niet waarom de medewerkers ICT ons deze antwoorden hebben gegeven. Het zou bijvoorbeeld zo kunnen zijn dat medewerkers ICT, vanwege hun ICT-kennis, preciezere manieren hebben om jonge cyberbreinen te herkennen in vergelijking tot ouders en docenten, waardoor de variabelen ‘Engelse taalbeheersing’ en ‘out of the box

denken' hen minder opvallen. Dergelijke redeneringen vallen echter buiten het domein van dit onderzoek.

4.3.2. Gematigde verschillen tussen controlegroep en andere groepen

De tweede categorie variabelen laten aan ons zien dat er bij de controlegroep een lagere uitkomst is dan bij de andere groepen, maar dat deze verschillen redelijk klein zijn. Met redelijk kleine verschillen bedoelen we verschillen die kleiner zijn dan 1 punt tussen één van de groepen en onze controlegroep. De variabelen waarbij dit aan de orde is zijn “Het hebben van veel online contacten”, “Het hebben van hyperfocus”, “Apparaten uit elkaar halen”, “Sterke analytische vaardigheden” en “Het hebben van een oog voor detail”.

Bij deze variabelen valt het dus op dat jonge cyberbreinen weliswaar onderscheidend zijn, maar dat deze onderscheiding marginaal is in verhouding met de controlegroep. Daarnaast valt het op dat het doorgaans de medewerkers ICT zijn die zorgen voor een verlaging van de aanvankelijke variabelen die gebruikt worden om jonge cyberbreinen te herkennen. Wederom komt dus de vraag naar boven: ‘Waarom zien we een verschil tussen de gegevens van medewerkers ICT en de andere groepen (docenten; ouders; volwassen ethische hackers)?’.

4.2.3. Grote verschillen tussen controlegroep en andere groepen

Bij deze variabelen valt het op dat jonge cyberbreinen onderscheidend zijn van de controlegroep, en dat deze verschillen groot zijn in vergelijking met de controlegroep. De variabelen waarbij dit het geval was, zijn “Nieuwsgierigheid in techniek”, “Interesse en kennis van computers”, “Weet snel hoe technische dingen werken en helpt de leerkracht” en “Veel kennis van digitale systemen”.

Het is voor een deel logisch te beredeneren waarom deze variabelen uitsteken ten opzichte van de andere variabelen. Deze vier variabelen betreffen variabelen die hun toespitsing vinden in techniek, wat logisch aansluit bij het profiel van een jong cyberbrein. Daarnaast valt het niet uit te sluiten dat medewerkers ICT simpelweg onnauwkeurige antwoorden geven omdat ze de jonge cyberbreinen waarmee ze in contact zijn niet goed genoeg kennen om alle variabelen goed genoeg te kunnen observeren bij deze cyberbreinen. Bij deze vier variabelen is het plausibel om aan te nemen dat alle groepen die we hebben ondervraagd aardig goed zijn in het observeren van deze variabelen, omdat deze variabelen meer onderscheidend zijn in vergelijking met de andere variabelen die we hebben gebruikt in ons onderzoek.

4.4. Aanvullende kenmerken en suggesties van respondenten

In het onderzoek hebben we een selectie gemaakt in de praktische kenmerken die we hebben getoetst, en hebben we ook onze respondenten de mogelijkheid gegeven om ontbrekende kenmerken en andere suggesties aan te dragen die we kunnen meenemen in het onderzoek.

4.4.1. Aanvullende kenmerken

Ouders noemden onder andere het ter discussie stellen van onlogische regels en creativiteit als belangrijke eigenschappen van jonge cyberbreinen. De volwassen hackers gaven ook extra kenmerken aan, zoals antiautoritair gedrag in hun kindertijd en autodidactische leerstijlen, wat suggereert dat deze jongeren vaak zelfsturend zijn in hun leerprocessen. Bovendien werd er een sterke nadruk gelegd op het creëren van eigen projecten, zoals het hacken van games. Volwassen hackers identificeerden ook kenmerken zoals “anti-autoritair gedrag” en “autodidactische leerstijlen”, wat suggereert dat de persoonlijke en sociale context van de jongeren een belangrijke rol speelt in hun ontwikkeling.

Samenvattend komen deze aanvullende kenmerken naar voren namelijk “Eerlijkheid in alle contexten en een sterk gevoel voor rechtvaardigheid”, “De neiging om onlogische regels of systemen ter discussie te stellen”, “Een autodidactische leerstijl, waarbij de jongeren zelfstandig nieuwe vaardigheden leren en technische problemen oplossen”, “Een voorliefde voor puzzels en complexe

uitdagingen” en een “Een actieve interesse om zelf technische oplossingen te creëren of bestaande technologieën na te bouwen.”. Een voorbeeld van het laatste kenmerk is te vinden in Bijlage 7.

4.4.2. De aanvullende kenmerken en de controlegroep

Uit het onderzoek zijn een aantal aanvullende kenmerken naar voren gekomen die jonge cyberbreinen ook lijken te kenmerken.

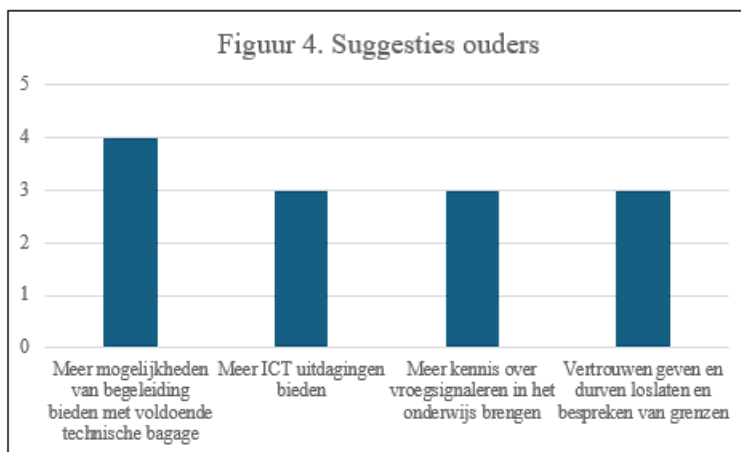
Om te onderzoeken in hoeverre deze aanvullende kenmerken uitsluitend van toepassing zijn op jonge cyberbreinen hebben we deze kenmerken ook aan de controlegroep voorgelegd. De vraag die we de controlegroep stelden was in hoeverre deze aanvullende kenmerken van toepassing zijn op hun eigen kind. Wat volgt is een korte bespreking van deze resultaten. Eerlijkheid kreeg een 3.63/5. De neiging om onlogische regels ter discussie te stellen krijgt een 3.50/5. Beide resultaten zijn logisch als je bedenkt dat ouders doorgaans het goede zien in hun kinderen, wat een verklaring kan zijn waarom ouders geloven dat hun kinderen (altijd) eerlijk zijn. Het ter discussie stellen is tevens iets wat de meeste kinderen doen.

Te zien is dat het hebben van een autodidactische leerstijl (2.50/5), het hebben van een voorliefde voor puzzels (2.06/5), en het hebben van een actieve interesse om zelf technische oplossingen te creëren (2.06/5) lager scoorden. Dit resultaat betekent dat deze drie aanvullende kenmerken wel door onze onderzoeksgroepen zijn opgemerkt als kenmerkend voor jonge cyberbreinen, en niet voor ouders van normale kinderen.

4.4.3. Suggesties van respondenten voor het helpen van jonge cyberbreinen

De respondenten hebben een breed scala aan suggesties gedaan wanneer wij aan hen vroegen wat goed zou zijn voor jonge cyberbreinen, en wat jonge cyberbreinen nodig zouden hebben in hun ontwikkeling.

Ouders benadrukken de noodzaak van erkenning voor de unieke leerstijl van jonge cyberbreinen. Zij stellen dat deze erkenning essentieel is voor de talentontwikkeling van hun kinderen. Er zijn verschillende suggesties gedaan, waaronder meer educatie voor ouders en leerkrachten, het creëren van ruimte voor zelfstudie, en begeleiding door technisch onderlegde personen.



Een kenmerkende uitspraak hierbij van een ouder op de vraag wat nodig zou zijn was “*Iemand die hem kon helpen in plaats van doorverwijzen. Maar er bestaat vrijwel geen dagbesteding. En hulp die wordt aangedragen heeft vaak niet voldoende technische bagage. Waardoor onze zoon er alsnog niks mee opschiet.*”

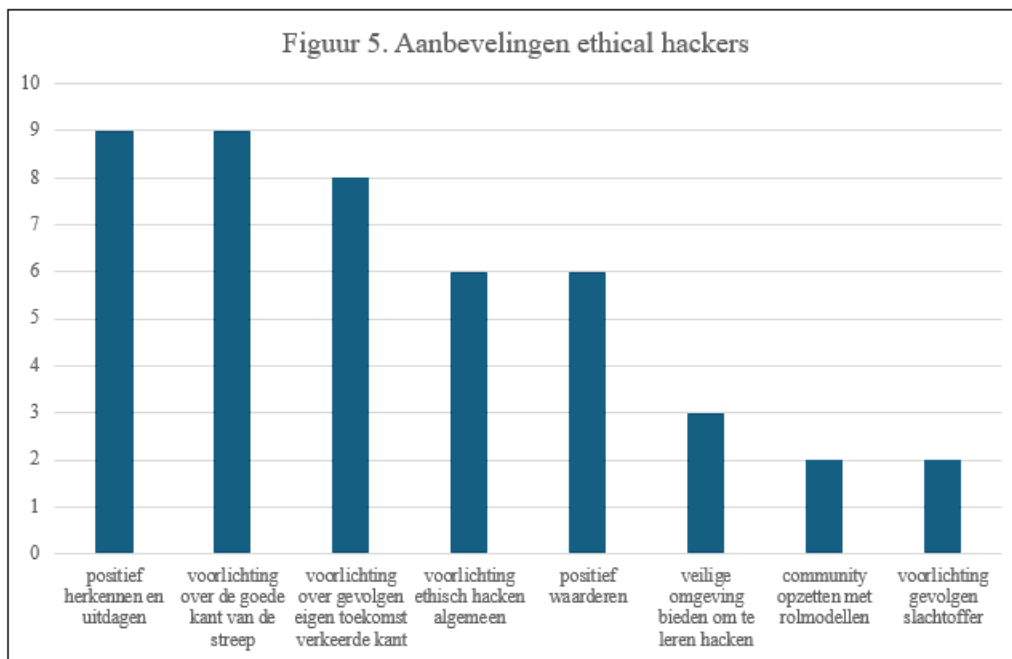
Dit duidt op een brede behoefte aan ondersteuning en begrip van de unieke kwaliteiten van deze jongeren, en de noodzaak om het onderwijs aan te passen aan hun specifieke behoeften. Ethical hackers hebben ook kritiek geleverd op het huidige schoolsysteem, dat onvoldoende ruimte biedt voor leerlingen die anders zijn en niet genoeg mogelijkheden biedt om digitale interesses te verkennen. Dit roept vragen op over de inclusiviteit van het onderwijs en de mogelijkheden die het biedt voor leerlingen met unieke talenten en interesses op hackgebied.

Vertrouwen geven noemde een ouder ook expliciet in een antwoord: *“Ik heb wel geleerd dat het ondanks de jonge leeftijd (8 jaar) heel belangrijk is om je kind vertrouwen te geven en “los” te laten zodat de enorme behoefte aan autonomie enigszins ingevuld kan worden.”*

Het vroeg leren (h)erkennen wordt ook genoemd als belangrijk getuige deze uitspraak van een ethical hacker: *“spot ze in de beginnende fase. Voordat vrienden of (cyber)criminelen hier misbruik van gaan maken. Ik denk zelf dat je i.p.v. straf erkenning moet geven en moet inspelen op de goede eigenschappen die al gespot kunnen worden.”*

Daarnaast benadrukten **medewerkers ICT** het belang van een integrale aanpak. Ze pleiten voor een samenwerking tussen scholen en jonge cyberbreinen, waarbij deze jongeren een actieve rol kunnen spelen, bijvoorbeeld door bij te dragen aan de beveiliging van hun schoolomgeving. Het gebrek aan een uniform beleid voor de begeleiding van deze jongeren werd ook opgemerkt, wat suggereert dat er behoefte is aan meer gestructureerde ondersteuning.

Hoewel de jonge cyberbreinen zelf niet zijn bevraagd, gaven de **ethical hackers** aan dat het leren (h)erkennen van hun talenten en vaardigheden, zoals leren programmeren, belangrijke behoeften zijn. Als onderdeel van een community: *“Wat belangrijk voor jongeren is, is om ze een gevoel van zelfwaarde te geven op een leuke manier wat ook moraal aanleren. Gezien kinderen nog veel moeten leren over de wereld en het moraal, is het makkelijk voor ze om van het pad af te gaan, maar niet als ze de juiste begeleiding krijgen, maar ook dat ze op positieve manier gestimuleerd worden met hun "talenten". Erbij willen horen is een belangrijk iets voor kinderen.”*



Het hebben van rolmodellen in een community werd ook vaker genoemd door ethical hackers als een belangrijke behoefte voor jonge cyberbreinen.

Voorlichting over de mogelijkheden aan de goede kant van de streep werden ook vaak door ethical hackers (9) genoemd evenals het geven van voorlichting over de gevolgen voor de eigen toekomst als je aan de criminele kant op gaat. Hierbij horen ook passende uitdagingen om het talent van een jong cyberbrein verder te ontwikkelen. Een ethical hacker merkte op dat *“voorlichting op scholen vanaf groep 6/7 zou hierbij kunnen helpen. Zonder waardeoordeel de risico's en gevaren van cybercriminaliteit benadrukken. Met name op het effect van de slachtoffers. Als je daartegenover het leuke van ethisch hacken belicht zou je in een vroeg stadium de jeugd al kunnen motiveren om aan de goede kant van de streep te blijven.”*

Door passende uitdagingen te geven kan je het gevoel van eigenwaarde vergroten aldus deze ethical hacker: *“Laat ze trots worden op iets dat ze 'maken' i.p.v. iets dat ze 'breken'. Een CVE hebben*

gemaakt/ontdekt is prima, een machine down krijgen is minder 'makend'. Breken is vaak de eerste stap, maar de echte faam en endorfine zit hem in het aanzien van een oplossing maken."

Wat ook uit het onderzoek naar voren kwam bij de diverse ondervraagde doelgroepen, dat jonge cyberbreinen vooral niet-criminele intenties lijken te hebben bij hacken. Nieuwsgierigheid, *"Vooral nieuwsgierigheid, Vooral de spanning of het lukt"*, gezien willen worden, uitdagingen zoeken, willen leren en bezorgdheid om de digitale veiligheid van bijvoorbeeld de school zijn de overwegende motieven die uit de antwoorden van onder andere ouders (10) naar voren kwamen. Of bijvoorbeeld van deze ethical hacker die aangaf: *"ik zou veel baat gehad kunnen hebben aan iemand die mijn nieuwsgierigheid niet onderdrukte of wegwimpelde, maar juist ging onderzoeken en bevorderen."*

Naast bovengenoemde behoeftes is het opvallend hoe makkelijk het was om een groot aantal ethical hackers (45) zo ver te krijgen om de vragenlijst te invullen. Daarnaast zijn er veel hackers geweest die lange en uitgebreide antwoorden gaven wanneer hen daartoe de mogelijkheid werd gegeven. Dit wijst erop dat het onderwerp van dit onderzoek bij deze groep een gevoelige snaar raakt, en dat het dus een onderwerp is dat erg leeft onder deze groep.

Dat sluit ook aan bij opmerkingen over gepest worden en zich buitengesloten voelen die vanuit de ethical hackers vaker terugkwamen. Een voorbeeld: *"Ik was een loner. Het had mij geholpen als ik meer geaccepteerd zou worden."* Of *"Ik had persoonlijk veel baat gehad bij mensen die begrepen hoe ik in elkaar zat. Ik werd bestempeld als 'lui' en leraren vonden het maar lastig dat ik niet sociaal kon meekomen met klasgenootjes en altijd afgeleid was. Ik ervaarde pestgedrag, wat zich in mijn geval manifesteerde tot het 'hacken' (phishen) van klasgenootjes om het speelveld gelijk te trekken"*.

Ook werd vanuit de groep ethical hackers heel vaak aangeboden om jonge cyberbreinen te ondersteunen en als een soort mentor op te treden waar nodig.

Samenvattend betekenen deze reacties dat het nodig is dat de maatschappij op een andere manier gaat kijken naar jonge cyberbreinen, en dat we deze jonge cyberbreinen niet zien als een probleem, maar juist als een kans. Dit idee gaat hand in hand met het geven van voorlichting op scholen aan jongeren waarbij jongeren bewust worden gemaakt van het effect van cybercriminaliteit.

5. Discussie

Dit onderzoek had als doel te onderzoeken in hoeverre een set aan praktische kenmerken kan bijdragen aan de vroegsignalering van jong cybertalent in groep 7 en 8 van de basisschool. De resultaten laten zien dat bepaalde praktische kenmerken bruikbaar zijn voor vroegsignalering, terwijl andere kenmerken minder of helemaal niet onderscheidend lijken. Inmiddels heeft de Stichting Cyberbrein.nl op basis van de lijst met gedragskenmerken een eerste handleiding voor professionals ontwikkeld (Bijlage 9) en op 13 oktober 2024 gaf de teamcaptain van het Nederlandse team dat deel heeft genomen aan de European Cybersecurity Challenge in Turijn aan dat hij zich volledig herkende in de beschrijving van kenmerken zoals in de handleiding opgenomen (Bijlage 10).

Tegelijkertijd zijn er een aantal limitaties ten aanzien van de validiteit en betrouwbaarheid aan dit onderzoek die hieronder toegelicht worden en die nopen tot vervolgonderzoek.

Hiernaast geven de opgedane inzichten uit het onderzoek ook aanleiding tot een aantal aanbevelingen voor de praktijk.

5.1. Reflectie op de theorie

Dit onderzoek richt zich op de praktische toepasbaarheid van kenmerken van jonge cyberbreinen. We hebben literatuur gebruikt om deze kenmerken te identificeren en een eerste lijst opgesteld met praktische kenmerken. Tegelijkertijd toont bestaande literatuur aan dat de oorsprong van deze kenmerken genuanceerd en contextafhankelijk is. De praktische gedragskenmerken van jonge cyberbreinen (10-12 jaar) blijken grotendeels een vertaling van theoretische variabelen uit de literatuur. Dit onderzoek draagt bij aan het beter herkennen van deze talenten, een onderwerp waar nog weinig over bekend is. Daarnaast blijken er aanvullende kenmerken te zijn, vooral onder ethical hackers. Toch zijn er ook verschillen met bestaande onderzoeken. Sommige studies suggereren dat niet alle cyberbreinen een natuurlijke affiniteit met ethisch hacken hebben; sociale beïnvloeding speelt soms een grotere rol (Van der Wagen et al., 2019). Dit wijst erop dat omgevingsfactoren, technologie-toegang en sociale context cruciaal zijn voor het herkennen van cyberbreinen. Mogelijk moet het huidige theoretische model worden aangevuld met omgevingsinvloeden.

Psychologische kenmerken zoals autisme en introversie verdienen aandacht. Dit onderzoek heeft deze aspecten grotendeels buiten beschouwing gelaten, maar literatuur (Happé & Frith, 2006) suggereert dat bijvoorbeeld de detailgerichte cognitieve stijl van mensen met autisme kan bijdragen aan technische vaardigheden. Een ander kenmerk dat een relatie met autisme kan hebben is het sterke gevoel voor rechtvaardigheid en het ter discussie stellen van onlogische regels, zoals ook in de aanvullende kenmerken naar voren kwam. Dit suggereert ook een verband dat nader onderzoek verdient om meer zicht te krijgen op de relatie tussen kenmerken van autisme en het hebben van een cyberbrein. Dit kan resulteren in betere herkenning van een cyberbrein juist onder de jongeren met een aandoening in het autistisch spectrum.

Hoogbegaafdheid zou ook een rol kunnen spelen. Volgens Velsink (2016) manifesteert hoogbegaafdheid zich namelijk vaak al op jonge leeftijd, onder meer door kenmerken als een sterk analytisch vermogen, een snelle informatieverwerking, een intense nieuwsgierigheid en een kritische houding ten opzichte van regels en autoriteit. Deze eigenschappen vertonen duidelijke overeenkomsten met de gedragskenmerken die in dit onderzoek zijn geïdentificeerd bij jonge cyberbreinen. Hoogbegaafde kinderen laten vaak een diepe interesse zien in specifieke onderwerpen en kunnen zich daarin op autodidactische wijze ontwikkelen. Wanneer deze interesse zich richt op technologie, netwerken of het oplossen van complexe digitale puzzels, ontstaat een overlap met het profiel van een jong cyberbrein. De intensiteit waarmee zij zich vastbijten in technische uitdagingen, hun behoefte aan autonomie, en hun neiging om systemen te willen doorgronden en verbeteren, zijn gedragspatronen die in beide profielen zichtbaar zijn. Daarnaast zijn hoogbegaafde kinderen vaak gevoelig voor rechtvaardigheid en logica, wat kan verklaren waarom sommige cyberbreinen hun handelen als 'gerechtvaardigd' zien, ondanks dat dit gedrag in juridische zin soms over de grens gaat. Dit onderstreept het belang van passende begeleiding: niet alleen op cognitief niveau, maar ook op sociaal-emotioneel vlak en op het gebied van ethiek. Hoewel niet elk cyberbrein per definitie hoogbegaafd is, en niet elke hoogbegaafde zich tot hacker ontwikkelt, is het zinvol om alert te zijn op deze mogelijke

samenhang. Een goed begrip van de dynamiek tussen hoogbegaafdheid en digitaal talent kan helpen om interventies beter af te stemmen op de behoeften van deze jongeren, zodat hun potentieel in veilige, constructieve banen geleid wordt.

In aanvulling hierop is theorie rond ethische ontwikkeling goed om hier te benoemen omdat het een belangrijke rol kan spelen in het begrijpen en begeleiden van jonge cyberbreinen. Volgens de morele ontwikkelingsleer van Kohlberg (Isaksson, 1979) doorloopt een individu verschillende stadia van morele ontwikkeling, waarbij het oordeel over wat 'goed' of 'fout' is steeds complexer en autonomer wordt. Kohlberg stelt dat deze ontwikkeling beïnvloedbaar is door externe factoren zoals opvoeding en onderwijs. Dit betekent dat moreel redeneren geen vaststaand gegeven is, maar in hoge mate gevormd en versterkt kan worden via educatie, interactie en begeleiding. Dit is bijzonder relevant in het kader van jonge cyberbreinen, omdat zij vaak over een grote technische vaardigheid beschikken, maar tegelijkertijd nog midden in hun morele ontwikkeling zitten. In de praktijk blijkt dat deze jongeren soms handelen vanuit nieuwsgierigheid of uitdaging, zonder zich volledig bewust lijken van de ethische implicaties van hun digitale gedrag.

Verscheidene onderwijs- en leertheorieën bieden ook handvatten om jonge cyberbreinen beter te herkennen en ontwikkelen. Constructivisme (Piaget, 1952) stelt dat leren ontstaat door actieve kennisopbouw, terwijl Vygotsky's Zone van naaste ontwikkeling (1978) het belang van begeleiding door mentoren benadrukt. Cyberbreinen leren vaak zelfstandig en verdiepen zich via online communities en hackingforums. Bruner (1966) stelt dat leren effectiever is in sociale contexten, wat aansluit bij gamified learning via zogenaamde Capture The Flags (Švábenský et al., 2020) en differentiatie in onderwijs (Tomlinson, 2001). Ook de Self-Determination Theory (Deci & Ryan, 2015) benadrukt dat autonomie en erkenning de motivatie verhogen. Het Differentiated Model of Giftedness and Talent (Gagné, 2004) onderstreept dat talentontwikkeling afhankelijk is van omgevingsfactoren.

Een andere invalshoek is het belang van culturele percepties van talentherkenning. Onderzoek van Leeman en Ledoux (2003) toont aan dat interculturele pedagogiek kan bijdragen aan een inclusieve talentherkenning. Ford (1998) en Varma (2006) benadrukken hoe culturele percepties en vooroordelen talentherkenning kunnen beïnvloeden. Dit onderstreept het belang van een inclusieve benadering voor het herkennen van cyberbreinen met een bi-culturele achtergrond.

Inclusiviteit die ook betrekking heeft op het onderscheid tussen jongens en meisjes. In de literatuur wordt benadrukt dat sekse een belangrijke rol speelt in hoe interesse in technologie zich ontwikkelt. Meisjes worden mogelijk minder vaak herkend als 'cyberbrein', doordat zij minder gestimuleerd worden of zichzelf minder snel identificeren met het bestaande beeld van een ICT-talent. Dit betekent dat signaleringslijsten, hoe objectief ze ook lijken, onbedoeld sekse specifieke biases kunnen bevatten. Cheryan et al. (2017) stellen dat culturele factoren zoals stereotypering, het gebrek aan vrouwelijke rolmodellen en de 'geeky' reputatie van sommige ICT-domeinen meisjes kunnen ontmoedigen om zich te ontwikkelen in deze richting. Dit onderstreept het belang van het ontwikkelen van een inclusieve benadering bij vroegsignalering van cybertalent.

Tot slot kan criminologische literatuur nadere inzichten bieden. Routine Activity Theory (Cohen & Felson, 1979) en Social Learning Theory (Akers, 1998) laten zien hoe bepaalde gedragsfactoren crimineel gedrag voorspellen. Onderzoek van Van der Wagen et al. (2021) suggereert dat sociale netwerken van cybercriminelen en traditionele criminelen overeenkomsten vertonen. Daarnaast kan Desistance Theory (Maruna, 2001) verklaren waarom jongeren hun criminele traject verlaten. Door deze criminologische inzichten te integreren, kunnen preventieve interventies en vroegsignalering verbeterd worden.

5.2. Reflectie op de methode: betrouwbaarheid en validiteit

De gekozen methode combineert academische onderbouwing met praktische toepassing in de onderwijssector. Dit biedt een unieke invalshoek, doordat theoretische inzichten worden getoetst binnen de Nederlandse onderwijscontext.

Desondanks zijn er methodologische beperkingen die de validiteit en betrouwbaarheid beïnvloeden. Zo is het aantal geïnterviewde docenten beperkt (n=7), wat kan leiden tot een verhoogde kans op anekdotisch bewijs. Daarnaast is niet onderzocht of bijvoorbeeld demografische kenmerken van respondenten van invloed kunnen zijn op de antwoorden. Toekomstig onderzoek zou deze

demografische factoren (zoals stedelijke omgeving/platteland, inkomen, gezinssituatie en opleidingsniveau ouders) moeten meenemen om de context verder te duiden. Dit kan weer invloed hebben op ontwerpkenmerken van interventies.

Een andere beperking betreft de ambiguïteit in gebruikte begrippen, zoals "groot rechtvaardigheidsgevoel" en "eerlijkheid in alle contexten", die voor verschillende respondenten op uiteenlopende manieren kunnen worden geïnterpreteerd. Ouders van jonge cyberbreinen kunnen een andere invulling geven aan deze termen dan ouders van "gewone" kinderen, afhankelijk van hun referentiekader. Dit kan resulteren in een vertekening van de resultaten, waarbij kenmerken mogelijk minder onderscheidend zijn dan beoogd.

Het onderzoek richt zich terecht op gedragskenmerken, maar een risico voor constructvaliditeit ontstaat door de nadruk op kenmerken zoals Engelse taalbeheersing en hyperfocus, die ook bij niet-cyberbreinen kunnen voorkomen. Dit werd bevestigd door de geringe verschillen met de controlegroep voor een aantal kenmerken. Een aanbeveling is om meer onderscheidende gedragskenmerken te ontwikkelen, eventueel met input van kinderpsychologen. Daarnaast is er een risico bij de theoretische vertaalslag van praktische kenmerken naar meetbare items in de vragenlijsten. Hoewel de kenmerken gebaseerd zijn op literatuuronderzoek, is de vertaling ervan naar concrete vragen niet altijd eenduidig. Hierdoor bestaat de mogelijkheid dat bepaalde eigenschappen niet volledig of nauwkeurig zijn gemeten, wat kan leiden tot een discrepantie tussen theoretische aannames en empirische resultaten. De onderlinge relatie tussen kenmerken is daarbij niet expliciet onderzocht. Sommige eigenschappen, zoals "oog voor detail" en "sterke analytische vaardigheden", vertonen overlap, wat kan leiden tot redundantie in de vragen en tot verwarring bij respondenten. Dit kan de interpretatie van de resultaten bemoeilijken en het onderscheidend vermogen van de kenmerken verminderen.

Verder kan de vraag gesteld worden 'wanneer is een kenmerk een goed kenmerk?'. Is dat zo wanneer het kenmerk daadwerkelijk een jong cyberbrein omschrijft? Of is dat zo wanneer het kenmerk een jong cyberbrein omschrijft, en wanneer zijn omgeving ook in staat is om een jong cyberbrein als zodanig te identificeren? Het gedane onderzoek sluit immers niet uit dat de praktische kenmerken die uit de literatuur komen niet kloppen, maar laat louter zien dat onze doelgroepen mogelijk wel moeite hebben met het gebruiken van deze (praktische) kenmerken.

Verder is bij volwassen ethische hackers retrospectief gevraagd naar hun ICT-vaardigheden in hun jeugd. Dit brengt het risico op recall bias met zich mee, omdat herinneringen mogelijk gekleurd zijn door latere ervaringen. De mate waarin deze antwoorden overeenkomen met de werkelijke situatie is daardoor lastig te verifiëren.

Daarnaast is in dit onderzoek is voor de meeste respondentengroepen een Likertschaal van 1 tot 5 gehanteerd, terwijl docenten de optie kregen om te antwoorden op een schaal van 0 tot 5. Dit verschil in antwoordopties heeft mogelijk geleid tot een systematische vertekening in de resultaten, aangezien docenten een extra lage antwoordmogelijkheid hadden die bij andere groepen niet beschikbaar was. Hierdoor kunnen de gemiddelde scores van docenten lager uitvallen, wat de vergelijkbaarheid tussen de groepen bemoeilijkt. Dit vormt een methodologische beperking van het onderzoek en dient in de interpretatie van de resultaten te worden meegenomen. In toekomstig onderzoek zou het aanbevolen zijn om voor alle groepen dezelfde schaal te hanteren om een betere onderlinge vergelijkbaarheid te waarborgen.

Ook wijken de scores van ICT-medewerkers af van de andere groepen, ondanks het gebruik van identieke vragen. Dit kan duiden op verschillen in testgroepen: de ouders van jonge cyberbreinen zijn niet per definitie de ouders van kinderen op de scholen waar deze ICT-medewerkers werken. Ook kan het verband houden met expertisebias: ICT-professionals herkennen mogelijk vooral technische kenmerken en hechten minder waarde aan andere signalen. Vervolgonderzoek is nodig om deze observaties nader te verklaren.

Een bijkomende beperking is de kans op responsbias, waarbij respondenten, met name ouders, sociaal wenselijke antwoorden hebben gegeven. Dit kan invloed hebben gehad op de mate waarin zij kenmerken zoals "behulpzaamheid" of "eerlijkheid" in hun kinderen herkennen, wat mogelijk leidt tot een overschatting van bepaalde eigenschappen.

Ook confirmation bias kan een rol hebben gespeeld, aangezien de vragenlijst is gebaseerd op bestaande literatuur en expertinput. Hierdoor is er een risico dat kenmerken zijn benadrukt die aansluiten bij eerdere aannames, zonder voldoende ruimte te bieden voor het ontdekken van nieuwe, mogelijk relevantere kenmerken. Dit kan de volledigheid en objectiviteit van de resultaten beperken.

De vergelijking met een controlegroep versterkt de interne validiteit. Echter, de onbedoelde afwijking in de schaal voor leerkrachten en de beperkte respons onder sommige groepen verzwakken de mogelijkheid om causale verbanden te trekken. Ook de selectie van ouders via re_B00TCMP kan een selectiebias veroorzaken, omdat deze ouders waarschijnlijk al bekend zijn met IT-vaardigheden van hun kinderen.

De resultaten zijn beperkt generaliseerbaar door de kleine steekproefgrootte bij leerkrachten en ICT-medewerkers. Daarnaast kan de context specifieke selectie van respondenten (zoals via re_B00TCMP) de representativiteit beperken. Een grotere, meer diverse steekproef zou de externe validiteit vergroten.

Bij docenten is gevraagd naar hun affiniteit met ICT, maar interpretatieverschillen kunnen een vertekening opleveren. Wat de ene docent als 'ICT-vaardig' beschouwt, kan sterk afwijken van hoe een ander dit definieert. Dit kan invloed hebben op de betrouwbaarheid van de resultaten, vooral omdat het aantal respondenten in deze groep beperkt is.

5.3. Praktische toepasbaarheid van de resultaten

Uit de resultaten blijkt dat er een aantal praktische kenmerken zijn die zeer goed aansluiten bij alle groepen, dat er een aantal praktische kenmerken die redelijk aansluiten bij de ondervraagde groepen, en dat er een aantal praktische kenmerken zijn die niet worden herkend en die door de controlegroep beter worden herkend dan door medewerkers ICT. Dit resultaat kan meerdere dingen betekenen.

Omdat de controlegroep bij een aantal variabelen hoger scoort dan de medewerkers ICT lijkt het erop dat deze variabelen minder geschikt zijn om jonge cyberbreinen te herkennen (de medewerkers ICT hebben deze variabelen immers niet herkend). Tegelijkertijd is het mogelijk dat de variabelen wel degelijk een voorspellende werking hebben (ze zijn immers niet voor niets in de literatuur opgenomen), maar dat medewerkers ICT specifiek minder goed zijn in het herkennen van jonge cyberbreinen op basis van deze specifieke variabelen.

Verder is er geen onderzoek uitgevoerd naar de kinderen van deze reguliere ouders, en is het een (geringe) mogelijkheid dat een deel van deze kinderen eveneens jonge cyberbreinen zijn. Het is aannemelijk dat dit niet het geval is, maar het is ook niet uit te sluiten, omdat we geen test hebben gedaan bij de kinderen van de ouders, en uitgaan van de expertise van de ouders.

Daarnaast zijn er een aantal variabelen in ons onderzoek die wel geschikt zijn om jonge cyberbreinen te identificeren, maar waarbij het verschil met de controlegroep minder groot dan 1 is. Dit betekent dat er onzekerheid is over de vraag hoe effectief deze variabelen daadwerkelijk zijn.

5.4. Aanbevelingen voor toekomstig onderzoek

Voor een verdere verfijning van vroegsignalering is een heldere operationalisering van kenmerken noodzakelijk. Dit betekent dat eenduidige definities en concrete voorbeelden ontwikkeld moeten worden om interpretatieverschillen tussen doelgroepen te minimaliseren. Daarnaast is het relevant om de onderlinge samenhang tussen kenmerken te analyseren: versterken ze elkaar, overlappen ze, of zijn ze juist onderscheidend?

Ook kan de methodologie verder worden verbeterd. Door vragen te herformuleren zodat elke vraag slechts één specifiek kenmerk meet, kan ambiguïteit worden verminderd. Daarnaast zou een kwantitatieve schaal voor gedragskenmerken kunnen worden geïntroduceerd, ondersteund door een grotere steekproef van leerkrachten en andere opvoeders. Dit verhoogt de objectiviteit en consistentie van de resultaten.

Een andere mogelijke beperking van dit onderzoek is de invloed van expertisebias. De bekendheid van de onderzoeker met cybersecurity kan onbewust hebben geleid tot een nadruk op bepaalde kenmerken, terwijl andere aspecten minder aandacht kregen. Dit kan resulteren in selectiebias, vooral bij open vragen, waarbij antwoorden die aansluiten bij de perceptie van de onderzoeker mogelijk prominenter worden meegenomen. Voor toekomstig onderzoek is het daarom van belang om maatregelen te nemen tegen deze bias, bijvoorbeeld door meerdere onderzoekers onafhankelijk van elkaar de data te laten analyseren.

Tot slot kan het gebruik van zelfrapportage via vragenlijsten de betrouwbaarheid van de resultaten beïnvloed hebben. Respondenten, vooral ouders en leerkrachten, kunnen gedragskenmerken op uiteenlopende manieren waarnemen en rapporteren. Dit kan worden opgevangen door aanvullende methoden te gebruiken, zoals gestructureerde interviews of directe observaties. Hierdoor kan de betrouwbaarheid van de bevindingen worden verhoogd en kunnen subjectieve interpretaties worden verminderd.

6. Conclusie

Dit onderzoek heeft aangetoond dat een set van praktische kenmerken uit de literatuur samengesteld kan worden en daarmee kan bijdragen aan het vroegtijdig herkennen van jonge cyberbreinen in groep 7 en 8 van de basisschool. De geïdentificeerde kenmerken bieden ouders, leerkrachten, ICT-medewerkers en andere betrokkenen een eerste handvat om digitaal talent bij jonge leerlingen te signaleren. Dit onderzoek biedt ook waardevolle inzichten in de herkenning van jonge cyberbreinen en de rol van verschillende betrokkenen daarbij. De resultaten hebben aan ons laten zien dat er verschillen zijn tussen de bruikbaarheid van de praktische kenmerken, omdat de controlegroep (ouders van normale kinderen) ook een deel van de variabelen terugzag bij hun eigen kinderen. Dit betekent dat er een aantal variabelen uit de literatuur een beperkte praktische toepasbaarheid hebben omdat de variabelen weliswaar aanwezig zijn bij deze kinderen, maar niet onderscheidend zijn van reguliere kinderen.

Samenvattend betekenen de resultaten dat jonge cyberbreinen het beste herkend kunnen worden aan indicatoren die technisch van aard zijn, omdat deze indicatoren onderscheidend zijn van andere kinderen en omdat het in de volle breedte van onze onderzoeksgroep voor de deelnemers mogelijk is om jonge cyberbreinen hieraan te herkennen. Dit kan beleidsmakers helpen om invulling te geven aan het identificeren van jonge cyberbreinen, wat kan helpen bij het herkennen van hun talent, het bieden van uitdagende leermogelijkheden en het ontwikkelen van de vaardigheden van jonge cyberbreinen.

Bij de andere variabelen waren er gematigde verschillen tussen de controlegroep en andere groepen, of zelfs grote verschillen. Het valt op dat de grote verschillen doorgaans zichtbaar zijn bij variabelen die technisch van aard zijn, en dat variabelen die meer psychologisch zijn minder onderscheidend zijn. Op basis van deze resultaten kunnen jonge cyberbreinen dus het beste herkend worden van andere kinderen op basis van de volgende praktische kenmerken: “Nieuwsgierigheid in techniek”, “Interesse en kennis van computers”, “Weet snel hoe technische dingen werken en helpt de leerkracht” en “Veel kennis van digitale systemen”.

6.1. Waarneming door verschillende groepen

Uit de praktijktoetsing blijkt dat ouders alle praktische gedragskenmerken vaker herkennen dan leerkrachten en ICT-medewerkers. Dit komt waarschijnlijk doordat ouders nauwer betrokken zijn bij het dagelijks gedrag en de ontwikkeling van hun kinderen. Leerkrachten hebben een beperkter zicht op de digitale vaardigheden en interesses van hun leerlingen, mogelijk door een lagere affiniteit met technologie. ICT-medewerkers kijken waarschijnlijk juist vooral vanuit een technisch perspectief, waardoor zij mogelijk niet altijd de bredere gedragskenmerken signaleren. Omdat leraren een andere vragenlijst kregen dan de andere groepen, valt niet uit te sluiten dat het geobserveerde verschil is ontstaan door de verschillende onderzoeksmethodes die zijn gehanteerd, in plaats van door de verschillende observaties van de groepen zelf.

6.2. Sociale en cognitieve aspecten

Naast technische en analytische vaardigheden laten jonge cyberbreinen vaak opvallende sociale en cognitieve kenmerken zien. Ze lijken een sterke drang te hebben om systemen en regels kritisch te analyseren en een sterk gevoel voor rechtvaardigheid tonen. Uit de antwoorden van volwassen ethische hackers bleek dat dit soms leiden tot frictie in traditionele onderwijssystemen, waar minder ruimte is voor zelfstandig en exploratief leren. Opvallend is dan ook dat veel ethische hackers en professionals in het veld aangaven dat zij zich als kind vaak buitengesloten voelden of met pestgedrag te maken hadden. Deze resultaten benadrukken het belang van een inclusieve en stimulerende omgeving voor jonge cyberbreinen.

6.3. Aanvullende kenmerken

Naast deze kenmerken heeft dit onderzoek ook aanvullende eigenschappen geïdentificeerd die waardevol kunnen zijn voor vroegsignalering. Deze aanvullende kenmerken omvatten “Eerlijkheid in alle contexten en een sterk gevoel voor rechtvaardigheid”, “De neiging om onlogische regels of systemen ter discussie te stellen”, “Een autodidactische leerstijl, waarbij de jongeren zelfstandig nieuwe vaardigheden leren en technische problemen oplossen”, “Een voorliefde voor puzzels en complexe uitdagingen” en een “Een actieve interesse om zelf technische oplossingen te creëren of bestaande technologieën na te bouwen.”.

Deze aanvullende kenmerken suggereren dat jonge cyberbreinen vaak meer dan alleen technisch vaardig zijn; ze vertonen ook sociaal en cognitief gedrag dat hen in staat stelt om problemen op unieke manieren aan te pakken. Dit roept de vraag op hoe het onderwijs en andere begeleidende instanties beter kunnen inspelen op deze kenmerken om het talent van jonge cyberbreinen optimaal te stimuleren en ontwikkelen.

6.4. Implicaties voor de praktijk en beleid

Uit de resultaten blijkt dat praktische kenmerken die technisch van aard zijn het makkelijkste zijn om jonge cyberbreinen aan te herkennen. Daarnaast blijkt uit de resultaten dat jonge cyberbreinen doorgaans kritisch zijn op regels en de behoefte voelen deze te breken. Hiermee zou het dus logisch zijn om te doen aan talentherkenning door middel van **Capture The Flag (CTF) evenementen**, omdat het jonge cyberbreinen in staat stelt om op een technische manier henzelf te onderscheiden en omdat objectief valt vast te stellen wanneer een deelnemer het goed heeft gedaan. Dit proces maakt herkenning makkelijk.

Volwassen ethische hackers gaven in de opmerkingen van de vragenlijsten aan dat ze erkenning van hun talenten misten toen zij zelf op school zaten, en dat een positieve stimulering van hun talenten had gelopen om hen op het rechte pad te houden. Met beide bevindingen in het achterhoofd is het logisch om **succesverhalen te delen** met als doel om jonge cyberbreinen te inspireren. Zie ook Bijlage 8 waarin een lagere school een flyer heeft opgehangen van een jong cyberbrein waarin hij zijn diensten aanbiedt op ICT-gebied. Dit kan worden georganiseerd in samenhang met het organiseren van **buitenlesactiviteiten en digitale uitdaging**, omdat dit jonge cyberbreinen de kans biedt om op een positieve manier hun talent in te zetten.

Het gevoel van volwassen hackers dat ze als buitenbeentje erkenning misten of niet de kans kregen om iets goeds te doen met hun talenten kan worden gezien als een breder probleem, waarbij een gebrek aan gemeenschapszin en mentoring een oorzaak is van het afglijden van deze jongeren. De oplossing daarmee ligt dan ook in het organiseren van **mentorschapsprogramma's en gemeenschapsvorming**.

Verder blijkt uit het onderzoek dat betrokkenheid een positieve relatie lijkt te hebben met de mogelijkheid om jonge cyberbreinen te signaleren, wat betekent dat het **vergroten van de ouderbetrokkenheid** tevens een goede suggestie is om de ontwikkeling van cyberbreinen te verbeteren.

Ook bleek uit de resultaten dat docenten zichzelf gematigd digitaal vaardig achten. De kans die hier ligt is om **leerkrachten en professionals te trainen**, met als doel om hen beter in staat te stellen om jonge cyberbreinen te herkennen en te begeleiden. Dit idee gaat in samenhang met het opstellen van **Responsible Disclosure-beleid op scholen**, waarbij cyberbreinen via een meldsysteem expliciet de mogelijkheid krijgen om hiaten te melden bij hun school, zonder de angst voor mogelijke represailles.

De bevinding dat praktische kenmerken van jonge cyberbreinen door verschillende doelgroepen verschillend worden herkend, wijst op een variatie in referentiekaders, kennisniveaus en dagelijkse interactie met de doelgroep. Ouders blijken bijvoorbeeld beter in staat om gedragskenmerken als nieuwsgierigheid of hyperfocus te herkennen, terwijl leerkrachten vaker aangeven moeite te hebben met het signaleren van deze kenmerken, mede wellicht vanwege hun lagere digitale affiniteit. ICT-medewerkers richten zich eerder op technische kennis. Ethische hackers daarentegen herkennen veel kenmerken uit hun eigen verleden. Deze verschillen vragen om een gedifferentieerde benadering in training en voorlichting: **Ouders** kunnen baat hebben bij trainingen die hen helpen om digitale interesse

bij hun kind te herkennen en positief te begeleiden. Hierin kan ook aandacht zijn voor ethiek, grenzen stellen en het bieden van uitdaging in een veilige context. Belangrijk is ook om hen handvatten te geven om in gesprek te gaan met school of hulpverlening.

Leerkrachten lijken meer behoefte aan bewustwordingstrainingen te hebben waarin praktische herkenningssignalen worden besproken aan de hand van concrete casussen. Daarnaast lijkt er een behoefte te bestaan aan het vergroten van hun digitale geletterdheid, zodat ze sneller signalen oppikken van digitale vaardigheden die verder gaan dan die van de gemiddelde leerling.

ICT-medewerkers kunnen meer toegespitste trainingen krijgen waarin de focus ligt op gedragspatronen die zich manifesteren binnen het digitale domein (zoals het zelfstandig oplossen van complexe problemen, het opzoeken van technische documentatie, het manipuleren van systemen) én hoe dit gedrag pedagogisch bespreekbaar gemaakt kan worden.

Ethische hackers en rolmodellen zouden kunnen worden ingezet in peer-to-peer trainingen of gastlessen waarin ze hun persoonlijke verhaal delen. In trainingen voor deze groep ligt de nadruk niet op herkenning, maar op hun rol als inspirator of mentor.

Differentiatie kan daarnaast plaatsvinden op een aantal manieren. Casus gestuurd leren, waarbij elke doelgroep leert aan de hand van herkenbare praktijksituaties uit hun eigen context. Ook het gebruik van persona's kan mogelijk helpen (bijvoorbeeld: "Jesse, 11 jaar, nieuwsgierig, verveeld in de klas, helpt de juf met de printer") om empathie te ontwikkelen voor het perspectief van het kind.

Door trainingsprogramma's te differentiëren per doelgroep, kan mogelijk de effectiviteit van vroegsignalering én de kans dat jonge cyberbreinen de juiste ondersteuning krijgen op het juiste moment vergroot worden.

Door deze aanbevelingen in de praktijk te brengen en verder onderzoek te doen naar de begeleiding van jonge cyberbreinen, kunnen we talent eerder herkennen en stimuleren in hun positieve ontwikkeling. Dit draagt bij aan zowel hun persoonlijke groei als aan een digitaal weerbare samenleving.

Hoe eerder een jong cyberbrein wordt herkend en ondersteund, des te groter de kans dat deze leerling zich begrepen voelt en zijn of haar talent op een constructieve manier kan inzetten. Dit kan voorkomen dat zij, zoals veel huidige ethische hackers in hun jeugd, te maken krijgen met sociale uitsluiting en onbegrip.

Dat moet veranderen: elk cyberbrein dat we op het rechte pad houden telt!

Literatuurlijst

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston, MA: Northeastern University Press.

Autoriteit Persoonsgegevens. (2024). Rapportage oktober 2024 [Report].

Bachmann, M. (2013). Deciphering the Hacker Underground. In IGI Global eBooks (pp. 175–194). <https://doi.org/10.4018/978-1-61350-323-2.ch112>

Bescherm je tegen cyberincidenten - Rabobank. (z.d.). Rabobank. <https://www.rabobank.nl/bedrijven/verzekeren/verzekeringsnieuws/bescherm-je-tegen-cyberincidenten>, geraadpleegd op 03-04-2025.

Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers? In *Cybercrime: Concepts, methodologies, tools and applications* (pp. 1499-1527). IGI Global.

Bruner, J. (1966). *Toward a Theory of Instruction*. Cambridge, MA: Harvard University Press.

Cheryan, S., Ziegler, S. A., Montoya, A. K., & Jiang, L. (2016). Why are some STEM fields more gender balanced than others? *Psychological Bulletin*, 143(1), pp. 1–35. <https://doi.org/10.1037/bul0000052>

Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), pp. 588-608.

CCV, Het (2023). Interventies op het gebied van Jeugd en cybercrime. Benaderd via: <https://hetccv.nl/app/uploads/2023/12/Interventies-op-het-gebied-van-Jeugd-en-Cybercrime-DEF-20231212.pdf> op 01-02-2024.

Deci, E.L. and Ryan, R.M. (2015) Self-Determination Theory. *International Encyclopedia of the Social & Behavioral Sciences*, 91, pp. 486-491. <https://doi.org/10.1016/B978-0-08-097086-8.26036-4>.

Derk-Admin. (2019, 9 augustus). 1 op de 6 Nederlandse jongeren heeft wel eens een cyberdelict gepleegd - Saferinternetcentre.nl. <https://www.saferinternetcentre.nl/1-op-de-6-nederlandse-jongeren-heeft-wel-eens-een-cyberdelict-gepleegd/>.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, 34, 165-172.

Europol, Internet Organised Crime Threat Assessment (IOCTA) (2024). © European Union Agency for Law Enforcement Cooperation

Ford, D. Y. (1998). The Underrepresentation of Minority Students in Gifted Education: Problems and Promises in Recruitment and Retention. *The Journal of Special Education*, 32(1), 4-14. <https://doi.org/10.1177/002246699803200102>

Gagné, F. (2004). Transforming gifts into talents: the DMGT as a developmental theory. *High Ability Studies*, 15(2), 119–147. <https://doi.org/10.1080/1359813042000314682>

Happé, F., Frith, U. (2006). The Weak Coherence Account: Detail-focused cognitive style in autism spectrum disorders. *Journal Of Autism And Developmental Disorders*, 36(1), pp. 5–25. <https://doi.org/10.1007/s10803-005-0039-0>

Henderson, V., Davidson, J., Hemsworth, K., & Edwards, S. (2014). Hacking the mastercode: Cyborg stories and the boundaries of autism. *Social & Cultural Geography*, 15(5), pp. 504-524.

Hirschi, T. (1969). *Causes of delinquency*. Berkeley: University of California Press.

Ísaksson, A. (1979). Kohlberg's Theory of Moral Development and Its Relevance to Education. *Scandinavian Journal Of Educational Research*, 23(2), pp. 47–63. <https://doi.org/10.1080/0031383790230202>

Kranenbarg, M. W., Van der Toolen, Y., & Weerman, F. (2022). Understanding cybercriminal behaviour among young people.

Kranenbarg, M. W., Van Gelder, J. L., Barends, A. J., & de Vries, R. E. (2023). Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in human behavior*, 140, 107576.

Kumar, I. (2023). Emerging threats in cybersecurity: a review article. *International Journal of Applied and Natural Sciences*, 1(1), pp. 01-08.

Kuner, C., Svantesson, D. J. B., H. Cate, F., Lynskey, O., & Millard, C. (2017). The rise of cybersecurity and its impact on data protection. *International Data Privacy Law*, 7(2), pp. 73-75.

Layman, L., Cornwell, T., Williams, L. A., & Osborne, J. (2005). Personality profiles and learning styles of advanced undergraduate computer science students. North Carolina State University. Dept. of Computer Science.

Leeman, Y., & Ledoux, G. (2003). Intercultural education in Dutch schools. *Curriculum Inquiry*, 33(4), pp. 385-399.

Lim, A., Brewer, N., & Young, R. L. (2023). Revisiting the relationship between cybercrime, autistic traits, and autism. *Journal of autism and developmental disorders*, 53(4), pp. 1319-1330.

Loggen, J., Moneva, A., & Leukfeldt, E. R. (2023). Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review.

Maruna, S. (2001). *Making good: How ex-convicts reform and rebuild their lives*. Washington, DC: American Psychological Association.

Ministerie van Justitie en Veiligheid. (2023, 3 juli). Cybersecuritybeeld Nederland 2023. Nationaal Coördinator Terrorismebestrijding en Veiligheid. <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland>.

Ministerie van Justitie en Veiligheid. (2024, 10 juni). CyberCrimebeeld (CCBN). Cybercrime | Openbaar Ministerie. <https://www.om.nl/onderwerpen/cybercrime/cybercrimebeeld-cybercrimebeeld-ccbn>.

NCSR. (2023, februari 16). Benaderd via:

<https://www.cybersecurityraad.nl/actueel/nieuws/2021/01/22/> geraadpleegd op 02-02-2024.

Noordegraaf, J. E., & Weulen Kranenbarg, M. (2023). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. *Criminology & Public Policy*, 22(4), pp. 803-824.

Odinot, G., De Poot, C., & Verhoeven, M. (2018). De aard en aanpak van georganiseerde cybercrime. *Justitiële Verkenningen*, 44(5), pp. 9–22. <https://doi.org/10.5553/jv/016758502018044005002>.

Payne, K. L., Russell, A., Mills, R., Maras, K., Rai, D., & Brosnan, M. (2019). Is there a relationship between cyber-dependent crime, autistic-like traits and autism? *Journal of Autism and Developmental Disorders*, 49, pp. 4159-4169.

Piaget, J. (1952). *The origins of intelligence in children*. New York: Norton.

re_B00TCMP. (z.d.). RE_B00TCMP. RE_B00TCMP. <https://re-b00tcmp.nl/>, geraadpleegd op 30-03-2024.

Seigfried-Spellar, K. C., O'Quinn, C. L., & Treadway, K. N. (2015). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour & Information Technology*, 34(5), pp. 533-542.

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2020). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, 102, 102154. <https://doi.org/10.1016/j.cose.2020.102154>.

Tollenaar, N., Beijers, J., Van der Laan, A. M., Wetenschappelijk Onderzoek- en Datacentrum. (2024). Monitor jeugd-delinquentie 2023. In Cahier (pp. 6–113). <https://repository.wodc.nl/bitstream/handle/20.500.12832/3385/Cahier-2024-14-volledige-tekst.pdf?sequence=9&isAllowed=y>.

Tomlinson, C. A. (2001). *How to Differentiate Instruction in Mixed-Ability Classrooms* (2nd ed.). Alexandria, VA: Association for Supervision and Curriculum Development (ASCD.)

UWV. (2020, mei). Factsheet_arbeidsmarkt_Overheid.pdf. Benaderd via: <https://www.cdho.nl>: https://www.cdho.nl/assets/uploads/2020/06/Factsheet_arbeidsmarkt_Overheid.pdf.

Varma, R. (2006). "Making computer science minority-friendly." *Communications of the ACM*, 49(2), pp. 129-134.

Velsink, M. (2016). Hoogbegaafdheid herkennen. *Kinderopvang*, 26(10), pp. 32–34. <https://doi.org/10.1007/s41189-016-0172-5>

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Cambridge, MA: Harvard University Press).

Van der Wagen, W., van't Zand-Kurtovic, E. G., & Fischer, T. F. C. (2019). Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin.

Van der Wagen, W., Fischer, T., Matthijsse, S., & Van 't Zand, E. (2021). Unique Offender, Unique Response? Assessing the Suitability and Effectiveness of Interventions for Cyber Offenders. In *Crime and justice in digital society* (pp. 371–390). https://doi.org/10.1007/978-3-030-60527-8_20.

Wagner, J., Bolgan, S., & Rusconi, E. (2022). On the relation between hacking and autism or autistic traits: A systematic review of the scientific evidence. *Cybersecurity and Cognitive Science*, pp. 157-196.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information systems management*, 24(4), pp. 281-287.

Zand, E., Matthijsse, S., Fischer, T., Wagen, W., Oerlemans, J. J., & Weulen Kranenbarg, M. (2020). Interventies voor cyber daders. *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk*, pp. 259-287.

Zebel, S., de Vries, P., Giebels, E., Kuttchreuter, M., & Stol, W. (2014). *Jeugdige daders van cybercrime in Nederland: een empirische verkenning*.

Bijlage 1: AI-statement

Tijdens dit onderzoek is er gebruik gemaakt van ChatGPT en AI functionaliteit van SCRIBBR. Het gebruik hiervan binnen dit onderzoek was strikt ondersteunend, en de resultaten zijn door mij zorgvuldig geverifieerd om de juistheid en betrouwbaarheid te waarborgen.

Het is gebruikt om:

- Exports van data uit Qualtrics in voorkomende gevallen samen te voegen en te analyseren en rekenkundige bewerkingen op uit te voeren waar nodig;
- Tekstsuggesties te doen voor zinnen die “niet lekker lopen”;
- Samenvattingen te maken van teksten om bondiger te formuleren;
- APA-check uit te voeren en suggesties voorstellen voor de juiste notatie en verwijzingen;
- Analyses te doen op resultaten om te komen tot suggesties voor samenvattingen/meest opvallende punten;
- Op basis van de onderzoeksresultaten een voorzet te doen voor suggesties voor aanbevelingen;
- Literatuurbronnen te analyseren en samen te vatten met als doel sneller te kunnen beoordelen of een bron relevant genoeg was om verder mee aan de slag te gaan.

De auteur benadrukt dat alle bevindingen en conclusies in dit onderzoek onafhankelijk zijn geformuleerd en dat de resultaten uit ChatGPT slechts een hulpmiddel waren ter ondersteuning van het onderzoeksproces.

Bijlage 2a: Vragenlijst Ouders jong cyberbrein

Start van blok: Introductie

Q1 U wordt uitgenodigd om deel te nemen aan een onderzoek met de titel "Jonge cyberbreinen vroeggesignaleerd". Dit onderzoek wordt uitgevoerd door Henk van Ee van de Faculteit Behavioural, Management and Social Sciences van de Universiteit Twente.

Het doel van dit onderzoek is om het talent van jonge cyberbreinen zo vroeg mogelijk leren herkennen. Met de resultaten van dit onderzoek kunnen we de jonge cyberbreinen hopelijk de juiste uitdagingen geven om hun talent verder te ontwikkelen en aan de goede kant van de streep te blijven en bedrijven en mensen helpen zo veilig mogelijk te zijn op digitaal gebied.

Doel van deze vragenlijst is om het profiel van een jong cyberbrein zoals dat uit de theorie komt, te toetsen in de praktijk en waar nodig aan te passen. En we denken dat u als ouder waardevolle input hiervoor heeft.

Uw deelname aan dit onderzoek is geheel vrijwillig en u kunt zich op ieder moment terugtrekken. Het staat u vrij om elke vraag achterwege te laten. Wij zijn van mening dat er geen bekende risico's verbonden zijn aan dit onderzoek. Zoals bij elke online-gerelateerde activiteit is het risico op een inbreuk echter altijd mogelijk. Binnen onze mogelijkheden zullen uw antwoorden in dit onderzoek vertrouwelijk blijven.

Wij minimaliseren eventuele risico's door de gegevens binnen de omgeving van de Universiteit Twente te houden en waar nodig te anonimiseren en binnen maximaal 2 maanden na afronding van het onderzoek te verwijderen.

Eventuele quotes zullen geanonimiseerd worden opgenomen in een eventuele publicatie. Nog vragen? Neem gerust contact op!

henk.van.ee@cyberbrein.nl of 06 42 158 182.

Het duurt ongeveer 20 minuten om het te voltooien.

Q9 Bij deze geef ik akkoord voor deelname en heb bovenstaande gelezen.

Ja (2)

Nee (3)

Pagina-einde

Profiel cyberbrein Uit de literatuur komt een beeld naar voren van het profiel van een jong cyberbrein. Dat is hieronder vertaald in een aantal (gedrags-)kenmerken zoals nieuwsgierigheid in techniek en heel veel kennis van ICT. Het gaat hierbij om feitelijk gedrag of eigenschappen die kunnen wijzen op een uniek talent.

In hoeverre zijn slaan die ook op uw zoon of dochter? Denk hierbij aan toen hij/zij op de basisschool zat of misschien nog zit.

	1	2	3	4	5
Heeft opvallend veel interesse in en kennis van computers en hoe ze werken ()					
Heeft opvallend veel kennis van digitale systemen (internet, netwerken) ()					
Is zeer nieuwsgierig in alles wat met techniek te maken heeft ()					
Heeft oog voor detail ()					
Heeft een hyperfocus om iets op te lossen en gaan door tot het is opgelost ()					
Weet snel hoe technische dingen werken en helpt leerkracht of anderen uit de directe omgeving hiermee ()					
Haalt apparaten en dingen uit elkaar halen om hun werking te zien ()					
Denkt Out of the box ()					
Beheerst de Engels taal goed ()					
Beschikt over sterke analytische vaardigheden ()					
Heeft veel online contacten en wat minder offline sociale contacten/relaties ()					

Q5 Mist u in de vorige vraag nog (gedrags-)kenmerken of specifieke eigenschappen die u opvallend vindt voor een jong cyberbrein en waar het talent nog meer aan herkend zou kunnen worden?

Pagina-einde

Q20 Hebben ze uw zoon/dochter herkend als "cyberbrein" op de lagere school en zo ja door wie?
meerdere antwoorden mogelijk

- ouders (1)
- leraar (2)
- medewerker ICT van de school (3)
- een andere volwassene (4)
- Anders namelijk: (5) _____
- Nee, hij/zij is niet herkend (6)

Q25 In hoeverre spelen de volgende redenen een rol voor een jongere om bezig te zijn met hacken op de lagere school denkt u?

- Vooral nieuwsgierigheid (4)
- Bezorgdheid om de digitale veiligheid van de school (5)
- "Erbij willen horen" en iets stoers laten zien (8)
- Vooral de spanning of het lukt (10)
- Anders namelijk (9) _____

Q24 Vraag: terugkijkend op de lagere schoolperiode van uw zoon/dochter: wat zou hij/zij aan extra begeleiding/uitdaging/informatie nodig hebben of hebben gehad?

Q10 Vraag: wat zou u als ouder nodig hebben om uw zoon/dochter goed te kunnen begeleiden?

Einde blok: Introductie

Start van blok: Een jong cyberbrein herkend en dan?

Q18 Heeft u verder nog tips/trucs hoe je het beste kunt omgaan met jonge cyberbreinen of andere feedback naar aanleiding van deze vragenlijst?

Einde blok: Een jong cyberbrein herkend en dan?

Bijlage 2b: Vragenlijst Ouders controlegroep

Start van blok: Introductie

Q1 U wordt uitgenodigd om deel te nemen aan een onderzoek met de titel "Jonge cyberbreinen vroeggesignaleerd". Dit onderzoek wordt uitgevoerd door Henk van Ee van de Faculteit Behavioural, Management and Social Sciences van de Universiteit Twente. Het doel van dit onderzoek is om het talent van jonge cyberbreinen zo vroeg mogelijk leren herkennen, al vanaf groep 7/8 van de basisschool. En het liefst voordat criminelen dit talent herkennen en actief inzetten voor allerlei vormen van cybercriminaliteit. Met de resultaten van dit onderzoek kunnen we de jonge cyberbreinen hopelijk veel eerder herkennen en de juiste uitdagingen geven om hun talent verder te ontwikkelen.

En om aan de goede kant van de streep te blijven en bedrijven en mensen helpen zo veilig mogelijk te zijn op digitaal gebied. Nu is er uit een eerdere stap in dit onderzoek een profiel met kenmerken van een jong cyberbreinen naar voren gekomen dat we graag willen voorleggen aan ouders van "gewone" kids.

Het doel van deze vragenlijst is om erachter te komen in hoeverre de kenmerken van een jong cyberbrein nu echt uniek zijn voor een cyberbrein of ook op andere jongeren slaan. Uw deelname aan dit onderzoek is geheel vrijwillig en u kunt zich op ieder moment terugtrekken. Het staat u vrij om elke vraag achterwege te laten. Wij zijn van mening dat er geen bekende risico's verbonden zijn aan dit onderzoek.

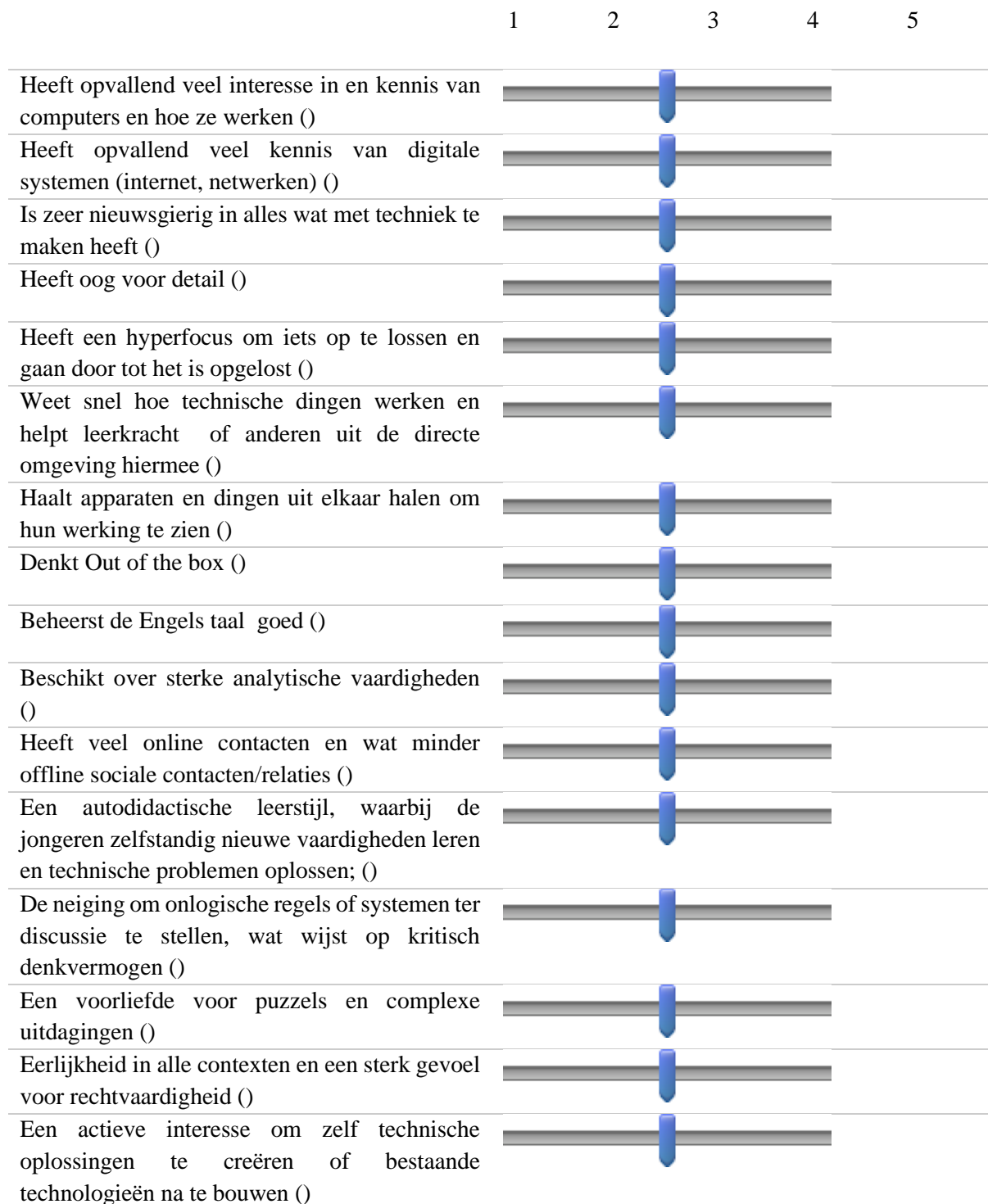
Zoals bij elke online-gerelateerde activiteit is het risico op een inbreuk echter altijd mogelijk. Binnen onze mogelijkheden zullen uw antwoorden in dit onderzoek vertrouwelijk blijven. Wij minimaliseren eventuele risico's door de gegevens binnen de omgeving van de Universiteit Twente te houden en waar nodig te anonimiseren en binnen maximaal 2 maanden na afronding van het onderzoek te verwijderen. Eventuele quotes zullen geanonimiseerd worden opgenomen in een eventuele publicatie. Nog vragen? Neem gerust contact op! henk.van.ee@cyberbrein.nl of 06 42 158 182. Het duurt ongeveer 5 minuten om het te voltooien.

Q9 Bij deze geef ik akkoord voor deelname en heb bovenstaande gelezen.

- Ja (2)
- Nee (3)

Pagina-einde

Profiel cyberbrein Uit de literatuur komt een beeld naar voren van het profiel van een jong cyberbrein. Dat is hieronder vertaald in een aantal (gedrags-)kenmerken zoals nieuwsgierigheid in techniek en heel veel kennis van ICT. In hoeverre slaan die ook op uw zoon of dochter toen hij/zij nog in groep 7/8 van de basisschool zat of zit? 1. Totaal niet herkenbaar 2. Redelijk onherkenbaar 3. Neutraal 4. Redelijk herkenbaar 5. Zeer herkenbaar



Einde blok: Introductie

Start van blok: Blok 1

Q12 Mocht u nog opmerkingen hebben, dan kan dat hieronder.

Einde blok: Blok 1

Bijlage 3: Vragenlijst medewerker ICT van een school

Start van blok: Introductie

Q1 U wordt uitgenodigd om deel te nemen aan een onderzoek met de titel Jonge cyberbreinen vroeggesignaleerd. Dit onderzoek wordt uitgevoerd door Henk van Ee van de Faculteit Behavioural, Management and Social Sciences van de Universiteit Twente. Het doel van dit onderzoek is om het talent van jonge cyberbreinen zo vroeg mogelijk leren herkennen. Het duurt ongeveer 20 minuten om het te voltooien.

Doel van deze vragenlijst is om het profiel van een jong cyberbrein zoals dat uit de theorie komt, te toetsen in de praktijk. En we denken dat u vanuit uw rol "veel ziet" op digitaal gebied op school en misschien wel nog meer kenmerkend gedrag ziet bij jonge cyberbreinen op uw school.

Daarna kunnen we de jonge cyberbreinen van nu hopelijk de juiste uitdagingen geven om hun talent verder te ontwikkelen en aan de goede kant van de streep te blijven: dus white hat hackers worden die bedrijven en mensen helpen zo veilig mogelijk te zijn.

De gegevens zullen worden gebruikt voor het toetsen van een set aan gedragskenmerken van een jong cyberbrein zoals dat uit de theorie naar voren is gekomen en die set aan te vullen met deze inzichten.

Uw deelname aan dit onderzoek is geheel vrijwillig en u kunt zich op ieder moment terugtrekken. Het staat u vrij om elke vraag achterwege te laten. Wij zijn van mening dat er geen bekende risico's verbonden zijn aan dit onderzoek.

Zoals bij elke online-gerelateerde activiteit is het risico op een inbreuk echter altijd mogelijk. Binnen onze mogelijkheden zullen uw antwoorden in dit onderzoek vertrouwelijk blijven. Wij minimaliseren eventuele risico's door de gegevens binnen de omgeving van de Universiteit Twente te houden en waar nodig te anonimiseren en binnen maximaal 2 maanden na afronding van het onderzoek te verwijderen.

Eventuele quotes zullen geanonimiseerd worden opgenomen in een eventuele publicatie.

Nog vragen? Neem gerust contact op! henk.van.ee@cyberbrein.nl of 06 42 158 182.

Q15 Bij deze geef ik akkoord voor deelname

Ja (1)

Nee (2)

Pagina-einde

Q3 Wat is het soort onderwijsinstelling waar u werkzaam bent?

- primair onderwijsgroep lager dan 7 (1)
 - primair onderwijsgroep 7/8 (2)
 - vmbo (3)
 - mbo (4)
 - mavo (5)
 - havo/vwo (6)
-

Q17 Hoeveel leerlingen heeft uw onderwijsinstelling totaal?

Pagina-einde _____

Profiel cyberbrein Uit de literatuur komt een beeld naar voren van het profiel van een jong cyberbrein. Een jong cyberbrein is een jongere die veel affiniteit met ICT heeft, nogal nieuwsgierig is en misschien al wel eens de onlinegrenzen opgezocht heeft.

Dat hebben we vertaald naar een aantal kenmerken. In hoeverre kloppen die kenmerken met het beeld dat u heeft van jonge cyberbreinen die mogelijk bij uw op school rondlopen?

	1	2	3	4	5
Heeft opvallend veel interesse in en kennis van computers en hoe ze werken ()					
Heeft opvallend veel kennis van digitale systemen (internet, netwerken) ()					
Is zeer nieuwsgierig in alles wat met techniek te maken heeft ()					
Heeft oog voor detail ()					
Heeft een hyperfocus om iets op te lossen en gaan door tot het is opgelost ()					
Weet snel hoe technische dingen werken en helpt leerkracht of anderen daarmee ()					
Haalt apparaten en dingen uit elkaar halen om hun werking te zien ()					
Denkt Out of the box ()					
Beheerst de Engels taal goed ()					
Beschikt over sterke analytische vaardigheden ()					
Heeft veel online contacten en wat minder offline sociale contacten/relaties ()					

Q18 Als u leerlingen voor de geest haalt die mogelijk aan een of meerdere gedragskenmerken voldoen en misschien wel een cyberbrein zijn, mist u dan nog concrete eigenschappen of gedragskenmerken in deze lijst?

Einde blok: Introductie






Start van blok: School en hacken

Q15 Heeft u zelf wel eens een of meerdere hack(pogingen) door een leerling meegemaakt?

- Omzeilen beveiligingsinstellingen van bijvoorbeeld de Chromebooks (1)
 - Username wachtwoord achterhaald van een leerkracht en gebruikt (2)
 - Wifi gehackt (3)
 - DDoS aanval uitgevoerd waardoor een systeem niet beschikbaar was (4)
 - Admin accountschool gevonden (5)
 - Illegaal spelletjes gedownload (6)
 - Anders namelijk (7) _____
-

Q19 In hoeverre bent u het eens met de volgende stellingen?

0 1 2 3 4 5

Leerlingen die op school digitale grenzen opzoeken verdienen straf ()	
Ik vind het eigenlijk best knap wat leerlingen soms kunnen om een schoolsysteem te hacken ()	
Ik zou graag jonge cyberbreinen inzetten om de school beter te beveiligen of doe dat al ()	
Leerlingen die op school digitale grenzen opzoeken verdienen vooral gewaardeerd te worden om hun talenten ()	
Verbieden en dichtzetten van allerlei systeemopties heeft niet zoveel zin bij een bepaalde categorie leerlingen want ze ontwijken die maatregelen toch wel ()	

Einde blok: School en hacken

Start van blok: Een jong cyberbrein herkend en dan?

Q12 Dit blok gaat over de situatie dat u een jong cyberbrein herkend heeft en hoe u en uw school er dan mee omgaan.

Q13 Heeft u school voor zover u weet een beleid als een leerling iets gehackt heeft en dat meldt?

Ja en dan kunnen ze zich melden bij: (1)

Nee (2)

Weet niet (3)

Q7 Stel u herkent een jong cyberbrein zonder dat hij/zij al iets gedaan heeft wat niet mag op digitaal gebied: wat doet u met zo'n leerling?

Schorsen en gesprek met ouders aangaan (5)

Altijd aangifte doen (6)

Vragen naar de motivatie van de leerling (8)

Anders namelijk: (9) _____

Q17 Hoe zou u het vinden als een cyberbrein gaat helpen om de ICT van de school veiliger te maken?

Geen goed idee, want (1) _____

Heel goed idee, want (2) _____

Weet niet/geen mening (3)

Q9 Heeft uw school mogelijkheden voor een jong cyberbrein voor extra begeleiding?

Q8 Kent u een of meerdere van deze initiatieven?

- Hackright (6)
- re_B00TCMP (7)
- Stichting Cyberbrein.nl (8)
- DIVD Academy (9)
- Nee (10)
- Nee maar wel.... (11) _____

Q14 Wat zou u nodig hebben om een jong cyberbrein goed te kunnen begeleiden?

Q18 Wat zou u verder nog kwijt willen over dit onderwerp wat niet aan de orde is gekomen in deze vragenlijst?

Einde blok: Een jong cyberbrein herkend en dan?

Bijlage 4: Vragenlijst Ethische Hacker

Start van blok: Introductie.

Q1 Fijn dat je wilt deelnemen aan dit onderzoek met de titel "Jonge cyberbreinen vroegesignaleerd". Dit onderzoek wordt uitgevoerd door Henk van Ee van de Faculteit Behavioural, Management and Social Sciences van de Universiteit Twente. Het doel van dit onderzoek is om het talent van jonge cyberbreinen zo vroeg mogelijk te leren herkennen. Daarna kunnen we de jonge cyberbreinen van nu hopelijk de juiste uitdaging en begeleiding bieden om hun talent verder te ontwikkelen en aan de goede kant van de streep te blijven: dus white hat hackers worden die bedrijven en mensen helpen zo veilig mogelijk te blijven.

Doel van deze vragenlijst is om het profiel van een jong cyberbrein zoals dat uit de theorie komt, te toetsen in de praktijk. In hoeverre herken jij je als ethical hacker in deze kenmerken toen je nog op de lagere school zat? En welke typische eigenschappen mis je misschien nodig? En wat zou jij nodig hebben gehad op de leeftijd van de basisschool?

Je deelname aan dit onderzoek is geheel vrijwillig en je kan zich op ieder moment terugtrekken. Het staat je vrij om elke vraag achterwege te laten. Wij zijn van mening dat er geen grote bekende risico's verbonden zijn aan dit onderzoek.

Zoals bij elke online-gerelateerde activiteit is het risico op een inbreuk op datagebied echter altijd mogelijk. Binnen onze mogelijkheden zullen je antwoorden in dit onderzoek vertrouwelijk blijven. Wij minimaliseren eventuele risico's door de gegevens binnen de omgeving van de Universiteit Twente te houden en waar nodig te anonimiseren. De gegevens worden uiterlijk twee maanden na afronding verwijderd.

Eventuele quotes zullen geanonimiseerd worden opgenomen in een eventuele publicatie.

En tot slot: misschien was de lagerschooltijd helemaal geen leuke tijd en heb je geen zin om daar weer uitgebreid over na te denken. Voel je vrij om dan niet mee te doen natuurlijk of om misschien wel fysiek af te spreken om erover te praten. Neem gerust contact op! henk.van.ee@cyberbrein.nl of 06 42 158 182.

Let op: je moet 16 jaar of ouder zijn om mee te kunnen doen aan deze vragenlijst.

Het duurt ongeveer 20 minuten om het te voltooien.

Q29 Ik ga akkoord met deelname en heb de tekst bij de introductie gelezen.

Ja (2)

Nee (3)

Pagina-einde

Q19 Wat is je leeftijdscategorie?

16-20 (1)

21-30 (2)

31-50 (4)

ouder dan 50 (5)

Pagina-einde

Profiel cyberbrein Uit de literatuur komt een beeld naar voren van het profiel van een jong cyberbrein. Dat is hieronder vertaald in een aantal kenmerken. In hoeverre sloegen die ook op jou toen je nog jong was en op de basisschool zat?

	1	2	3	4	5
Heeft opvallend veel interesse in en kennis van computers en hoe ze werken ()					
Heeft opvallend veel kennis van digitale systemen (internet, netwerken) ()					
Is zeer nieuwsgierig in alles wat met techniek te maken heeft ()					
Heeft oog voor detail ()					
Heeft een hyperfocus om iets op te lossen en gaan door tot het is opgelost ()					
Weet snel hoe technische dingen werken en helpt leerkracht of anderen uit de directe omgeving hiermee ()					
Haalt apparaten en dingen uit elkaar halen om hun werking te zien ()					
Denkt Out of the box ()					
Beheerst de Engels taal goed ()					
Beschikt over sterke analytische vaardigheden ()					
Heeft veel online contacten en wat minder offline sociale contacten/relaties ()					

Q5 Mis je in de vorige vraag nog cruciale eigenschappen of (gedrags-)kenmerken die je opvallend vindt voor een jong cyberbrein en die toegevoegd moeten worden volgens jou?

Q24 Vraag: terugkijkend op je lagere schoolperiode: wat zou je aan extra begeleiding/uitdaging/informatie nodig hebben gehad en van wie?

Einde blok: Introductie

Start van blok: School en hacken

Q15 Heb je zelf op de lagere school wel eens "digitaal kwattekwaad" uitgehaald?

- Nee (1)
- Ja, en dit heb ik gedaan: (2) _____

Q23 En als je "digitaal kattedkwaad" hebt uitgehaald op de lagere school, hoe werd er toen gereageerd?

- Alleen straf (1)
 - Je werd vooral positief benaderd (3)
 - Ik ben nooit betrapt (5)
-

Q25 In hoeverre speelden de volgende redenen bij jezelf of bij hackers die je kent een rol om actief te zijn met hacken op de lagere school denk je?

- Vooral nieuwsgierigheid (4)
 - Bezorgdheid om de digitale veiligheid (5)
 - "Erbij willen horen" en iets stoers laten zien (8)
 - Vooral de spanning of het lukt (10)
 - Anders namelijk (9) _____
 - Ik heb nooit gehackt op de lagere school (12)
-

Q26 Vraag: wat zijn volgens jou redenen waarom jonge cyberbreinen uiteindelijk in de (cyber)criminele hoek belanden?

- Snel geld verdienen (2)
- Sociale contacten krijgen/ergens bij willen horen (3)
- Gedwongen door (cyber)criminelen (4)
- Uit naïviteit mensen willen helpen (7)
- Vrienden die je vragen om mee te helpen (8)
- Anders namelijk (6) _____

Einde blok: School en hacken

Start van blok: Een jong cyberbrein herkend en dan?

Q18 Heb je verder nog tips om jonge cyberbreinen aan de goede kant van de streep te houden of zijn er nog andere opmerkingen die je wilt maken?

Bijlage 5: Vragenlijst Leerkracht

Start van blok: Introductie

Q1 Superfijn dat je mee wilt doen aan deze vragenlijst. De reden van dit onderzoek is dat we het talent van jonge cyberbreinen graag zo vroeg mogelijk willen herkennen. Met een cyberbrein wordt bedoeld dat iemand onder andere erg slim is, nieuwsgierig is naar techniek, veel affiniteit met ICT heeft en mogelijk al geïnteresseerd is in en bezig is met hacken.

We krijgen ook graag een beeld van de omvang: om hoeveel jonge cyberbreinen gaat het ongeveer? We hopen dat onder andere te doen door jou als docent te vragen naar je ervaringen.

Als vervolg op dit onderzoek kunnen we ze hopelijk de juiste uitdagingen geven om hun talent verder te ontwikkelen en aan de goede kant van de streep te blijven: dus hackers worden die bedrijven en mensen helpen zo veilig mogelijk te zijn.

Je deelname aan dit onderzoek is geheel vrijwillig, anoniem en je kan zich op ieder moment terugtrekken. Het staat je vrij om elke vraag achterwege te laten.

Wij zijn van mening dat er geen grote bekende risico's verbonden zijn aan dit onderzoek. Zoals bij elke online-gerelateerde activiteit is het risico op een inbreuk op datagebied echter altijd mogelijk. Binnen onze mogelijkheden zullen je antwoorden in dit onderzoek vertrouwelijk blijven.

Wij minimaliseren eventuele risico's door de gegevens binnen de omgeving van de Universiteit Twente te houden en waar nodig te anonimiseren. De gegevens worden uiterlijk twee maanden na afronding verwijderd. Eventuele quotes zullen geanonimiseerd worden opgenomen in een eventuele publicatie.

En tot slot: in de vragenlijst wordt ook gevraagd of je eventueel een verdiepende workshop zou willen met jonge cyberbreinen die je herkend hebt. Neem gerust contact op! henk.van.ee@cyberbrein.nl of 06 42 158 182. Dan bespreek ik graag de mogelijkheden.

Mocht je een concrete vraag of probleem hebben op het gebied van hackende leerlingen, je kan me altijd bellen! Ik denk graag mee!

Het invullen duurt maximaal 20 minuten.

Pagina-einde

Q3 Wat is het soort onderwijsinstelling waar u werkzaam bent?

- primair onderwijsgroep lager dan 7 (1)
 - primair onderwijsgroep 7/8 (2)
 - vmbo (3)
 - mbo (4)
 - mavo (5)
 - havo/vwo (6)
-

Q4 Wat is de leeftijd van de leerlingen in uw klas?







- jonger dan 8 (1)
 - tussen 8 en 11 (2)
 - ouder dan 11 en jonger dan 15 (3)
 - ouder dan 15 (4)
-



Q11 In hoeverre heeft u zelf kennis over de (online)wereld van een jong cyberbrein en bent u bekend met:

0 Geen kennis

0 1 2 3 4 5 6 7 8 9 10

Roblox ()	
Minecraft ()	
Discord ()	
GTA ()	
Flipper zero ()	
DDoS aanval ()	

Pagina-einde

Profiel cyberbrein Uit de literatuur komt een beeld naar voren van het profiel van een jong cyberbrein. In hoeverre kloppen die kenmerken met het beeld dat u heeft van een jong cyberbrein?

0 1 2 3 4 5

Heeft opvallend veel interesse in en kennis van computers en hoe ze werken ()	
Heeft opvallend veel kennis van digitale systemen (internet, netwerken) ()	
Is zeer nieuwsgierig in alles wat met techniek te maken heeft ()	
Heeft oog voor detail ()	
Heeft een hyperfocus om iets op te lossen en gaan door tot het is opgelost ()	
Weet snel hoe technische dingen werken en helpt leerkracht daarmee ()	
Haalt apparaten en dingen uit elkaar halen om hun werking te zien ()	
Denkt Out of the box ()	
Beheerst de Engels taal goed ()	
Beschikt over sterke analytische vaardigheden ()	
Heeft veel online contacten en wat minder offline sociale contacten/relaties ()	

Q22 Uit de vragenlijsten met Ethical Hackers en Ouders kwamen nog een aantal aanvullende gedragskenmerken die mogelijk wijzen op het hebben van een cyberbrein. In hoeverre herkent u deze?

0 1 2 3 4 5

Stelt dingen ter discussie, loopt niet zonder goede reden mee met systemen van de maatschappij of school ()	
Houdt erg van puzzels ()	
Is goudeerlijk ()	
Niet alleen interesse hoe dingen in elkaar zitten maar ook om zelf (na) te bouwen ()	

Q5 Mist u nog (gedrags-)kenmerken in de vorige 2 vragen die u echt opvallend vindt voor een jong cyberbrein?

Q20 Als u naar dit profiel kijkt en uw leerlingen "scant", hoeveel leerlingen zouden dan mogelijk het talent van een cyberbrein hebben per klas?

- 0 (13)
 - 1 (4)
 - 2 (5)
 - 3 (6)
 - 4 (7)
 - 5 (8)
 - 6 (9)
 - 7 (10)
 - 8 (11)
 - 9 (12)
-

Q21 Stel dat u een aantal jonge cyberbreinen herkent, zou u er open voor staan om met deze leerlingen en hun ouders in contact te treden om een verdiepende workshop te organiseren met deze jonge cyberbreinen? Doel is om te kijken in hoeverre het profiel en de "scan" kloppen.

- Ja (1)
- Nee (2)
- Weet ik nog niet (3)

Einde blok: Introductie

Start van blok: School en hacken.

Q15 Heeft u zelf wel eens een situatie meegemaakt waarin een leerling u of een collega gehackt heeft?

- Nee (1)
- Ja, en dit was gebeurd: (2) _____
- Weet niet (3)

Einde blok: School en hacken

Start van blok: Een jong cyberbrein herkend en dan?

Q12 Dit blok gaat over de situatie dat u een jong cyberbrein herkend heeft en hoe u en uw school er dan mee omgaan.

Q13 Heeft u school voor zover u weet een beleid als een leerling iets gehackt heeft en dat meldt?

- Ja en dan kunnen ze zich melden bij: (1)

 - Nee (2)
 - Weet niet (3)
-

Q7 Stel u herkent een jong cyberbrein: naar wie of wat zou u kunnen doorverwijzen?

- De medewerker ICT van de school (1)
- Een collega leerkracht (2)
- Anders _____ namelijk.... (3)
-

Q17 Hoe zou u het vinden als een cyberbrein gaat helpen om de ICT van de school veiliger te maken?

- Geen goed idee, want (1) _____
- Heel goed idee, want (2) _____
- Weet niet/geen mening (3)
-

Q8 Kent u een of meerdere van deze initiatieven?

- Hackright (6)
- re_B00TCMP (7)
- Stichting Cyberbrein.nl (8)
- DIVD Academy (9)
- Nee (10)
- Nee maar wel.... (11) _____
-

Q9 Heeft uw school extra begeleidingsmogelijkheden een jong cyberbrein?

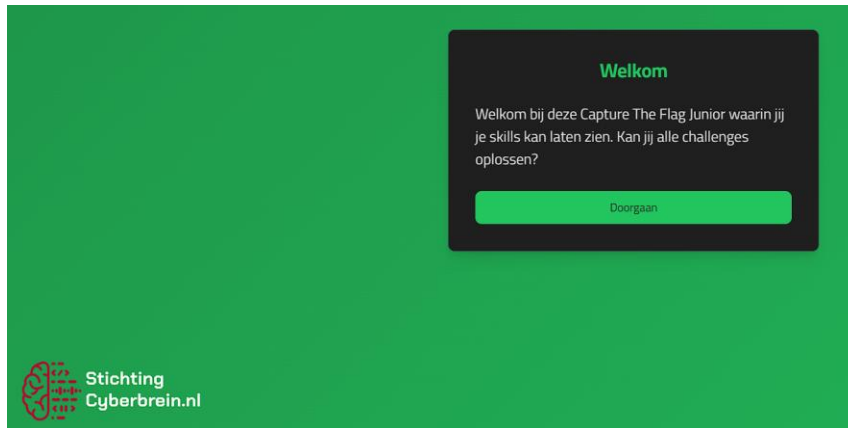
Q14 Wat zou u nodig hebben om een jong cyberbrein goed te kunnen begeleiden?

Q18 Wat zou u verder nog kwijt willen over dit onderwerp of nog andere suggesties/opmerkingen?

Einde blok: Een jong cyberbrein herkend en dan?

Bijlage 6: Capture The Flag Junior

Hieronder wordt beschreven uit welke opdrachten de Capture The Flag Junior bestaat om een beeld te krijgen van de kennis en vaardigheden van de deelnemer. Het zijn diverse opdrachten die gaan over computervaardigheden zoals onderwater in de HTML-code kijken tot eenvoudige encryptieopdrachten om kennis te toetsen.



De CTF bestaat uit 6 opdrachten in oplopende moeilijkheidsgraad.



Opdracht 1: uitleg over de CTF Junior via een opdracht

Introductie ×

In deze challenge krijg je uitleg over de Capture The Flag Junior zodat je snapt wat je moet doen! Heel veel plezier en succes!

Start

Heb je de flag gevonden? Vul deze hier in:

Controleer

Na klikken op Start:

Korte uitleg

Welkom bij de CTF, een Capture The Flag spel waarbij je verschillende opdrachten moet oplossen. De opdrachten zijn van verschillende niveaus, kun jij ze allemaal oplossen?

Alle flags zijn te herkennen aan het volgende formaat: `flag{}`

Hier heb je alvast de eerste flag, veel succes met de rest van de opdrachten!

```
flag{536d685152326c6b4d7a4a6d565468475
9324a725932597a4e586c4b646b35354b33644
e526d564f636d78325231517257475232656e7
0435554303d}
```

Opdracht 2: “onderwater kijken in de source code”

Gevoelige data

Het is altijd belangrijk om gevoelige data te beschermen. Probeer de flag te vinden.

Start

Heb je de flag gevonden? Vul deze hier in:

Vul hier de flag in

Controleer

Via rechtermuisklik en View Source page wordt de Flag zichtbaar en kan ingevuld worden.

```
<div class="newsletter-form">
  <h2>Abonneer op onze nieuwsbrief</h2>
  <form action="#" method="post">
    <input type="text" name="naam" placeholder="Je naam" required>
    <input type="email" name="email" placeholder="Je e-mailadres" required>
    <button type="submit">Aanmelden</button>
  </form>
</div>

<div class="hidden">
  <input type="hidden" name="auth_token" value="flag{6458673152537473563264434d573575565749724e55673162464672647a64535457394551336c79646a644e4f564e6962564a79526a5a5a5554303d}">
</div>

</div>
</main>

<footer class="bg-gray-900 text-white py-4 text-center">
  <p>Gemaakt met liefde door Joost Jansen &copy; 2024</p>
</footer>
</div>
```

Opdracht 3: “slechte wachtwoorden”

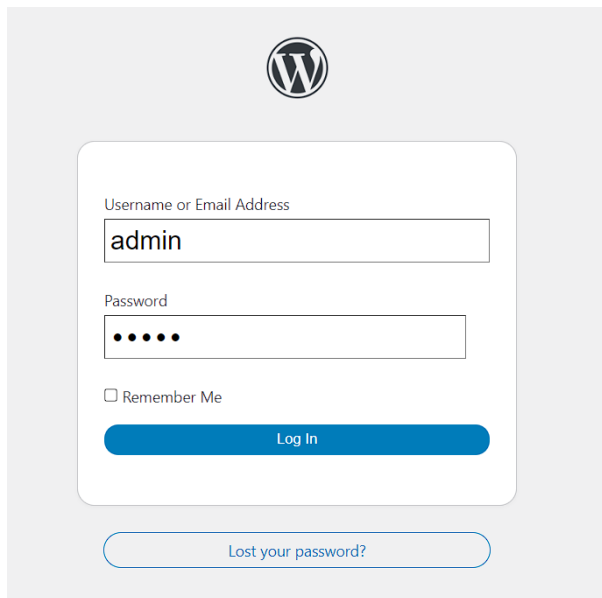
Slechte wachtwoorden

Jan heeft een admin omgeving gebouwd voor zijn blog en hij is hier super trots op! Helaas is Jan niet zo goed in het verzinnen van wachtwoorden. Kun jij inloggen bij de admin omgeving?

[Start](#)

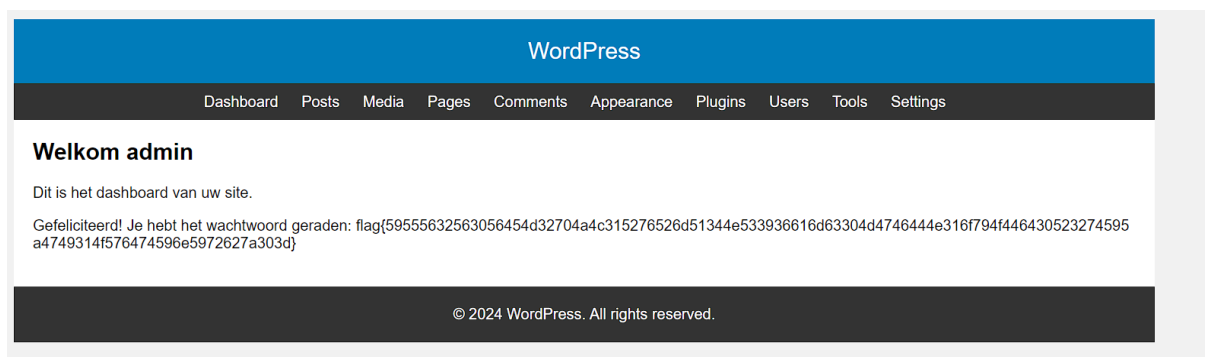
Heb je de flag gevonden? Vul deze hier in:

[Controleer](#)



The image shows the WordPress login interface. At the top is the WordPress logo. Below it is a white login box with a rounded border. Inside the box, there are two input fields: 'Username or Email Address' containing the text 'admin' and 'Password' with five dots. Below the password field is a checkbox labeled 'Remember Me' which is unchecked. At the bottom of the box is a blue 'Log In' button. Below the login box is a link that says 'Lost your password?'.

Invullen van admin admin levert de flag op:



The image shows a screenshot of the WordPress dashboard. At the top is a blue header with the word 'WordPress'. Below the header is a dark navigation bar with links for 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins', 'Users', 'Tools', and 'Settings'. The main content area has a white background and starts with the heading 'Welkom admin'. Below the heading is the text 'Dit is het dashboard van uw site.' followed by a congratulatory message: 'Gefeliciteerd! Je hebt het wachtwoord geraden: flag{59555632563056454d32704a4c315276526d51344e533936616d63304d4746444e316f794f446430523274595a4749314f576474596e5972627a303d}'. At the bottom of the dashboard is a dark footer with the text '© 2024 WordPress. All rights reserved.'

Opdracht 4: “slechte wachtwoorden een stap moeilijker: Encryptie”


Encryptie

Jan heeft zijn wachtwoord aangepast, maar zijn wachtwoord is gelekt op het internet en dit is het wachtwoord wat hij overal gebruikt. Kun jij iets met dit gelekte wachtwoord?

[Start](#)

Heb je de flag gevonden? Vul deze hier in:

[Controleer](#)



Beveiligd wachtwoord:
7e2feac95dcd7d1df803345e197369af4b156e4e7a95fcb2955bdbbb3a11afd8bb9d35931bf15511370b18143e38b01b903f55c5ecbded4af99934602fcdcf38c

Username or Email Address

Password

Remember Me

[Log In](#)

[Lost your password?](#)

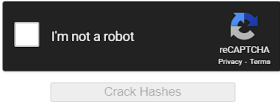
Het wachtwoord is een zogenaamde hash van een wachtwoord en moet via een online decryptietool ontsleuteld worden om daarna het plain text wachtwoord in te kunnen voeren.

Je kan hiervoor bijvoorbeeld Crackstation voor gebruiken:

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
7e2feac95dcd7d1df803345e197369af4b156e4e7a95fcb2955bdbbb3a11afd8bb9d35931bf
15511370b18143e38b01b903f55c5ecbde4af99934602fcd38c
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1{sha1_bin}), QubesV3.1BackupDefaults

Hash	Type	Result
7e2feac95dcd7d1df803345e197369af4b156e4e7a95fcb2955bdbbb3a11afd8bb9d35931bf15511370b18143e38b01b903f55c5ecbde4af99934602fcd38c	sha512	4321

Color Codes: **Green**: Exact match, **Yellow**: Partial match, **Red**: Not found.

Het wachtwoord is dus blijkbaar 4321 in dit geval en levert de flag op na invullen:

WordPress

[Dashboard](#) [Posts](#) [Media](#) [Pages](#) [Comments](#) [Appearance](#) [Plugins](#) [Users](#) [Tools](#) [Settings](#)

Welkom admin

Dit is het dashboard van uw site.

Gefeliciteerd! Je hebt het wachtwoord geraden: flag{5457317a4e3263305932396c4d335259617a4279616c7050626e55305231645559544a694e45784a656e464c516b46484c316732513049765754303d}

© 2024 WordPress. All rights reserved.

Opdracht 5: versleuteling via Rotation

In deze opdracht is een bericht versleuteld via de zogenaamde Rotation methode: elke letter verschuift een vast aantal posities in het alfabet.

In deze opdracht kan de deelnemer laten zien dat hij ook via Google bv. zoekt naar oplossingen.

The screenshot shows a web interface for a challenge. At the top, it says 'Versleutelde berichten' with a close button. Below that is a question: 'De meester op school dacht slim te zijn door een bericht naar de directeur onleesbaar te maken. Kan jij er uitkomen wat hij gestuurd heeft?'. There is a green 'Start' button. Below the question, it asks 'Heb je de flag gevonden? Vul deze hier in:' followed by a text input field with the placeholder 'Vul hier de flag in'. At the bottom, there is a green 'Controleer' button.

The screenshot shows a school website. On the left is a dark sidebar with 'Home', 'Berichten', and 'Instellingen'. The main content area is titled 'Regenboog Rivier School - Berichtenschermb' and contains a list of news items: 'Update over cijfers', 'Salaris verhoging vraag', and 'Huidige staat klas 7B'. Below this, there is a dark grey area with a list of items: 'Salaris verhoging vraag' and 'Huidige staat klas 7B'. At the bottom, there is a white notification box with a close button. The notification text reads: 'Vraag: Tbrqrvzqqnt zrarre U. Vx uro rra ierrzqr pbqr va zvwa qbphzrag ina h fgna: synt{546r4n5962457849546r46616132527561546p5n526p524r553238314p7n5n4s4q7n4r734s44647264455933567n5n6s596n56325n58566o637n303q}'.

In dit geval is de rotatie 13 en kan je via allerlei tools de verplaatsing terugdraaien:

rot13.com

[About ROT13](#)

```
Tbrqzvgqnt zrarr U. Vx uro rra ierrzqr pbqr va zvwa gbphzrag ina h fgna:  
synt{546r4n5962457849546r46616132527561546p5n526p524r553238314p7n5n4s4q7n4r734s446  
47264455933567n5n6s596n56325n58566o637n303q}
```

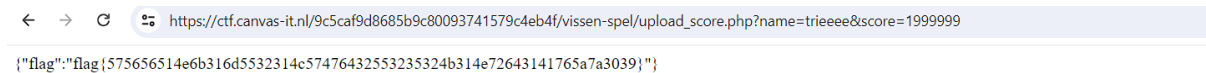
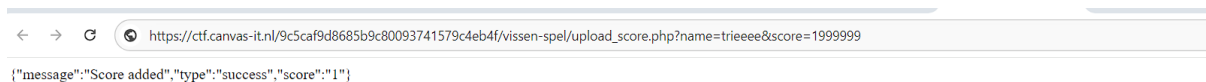
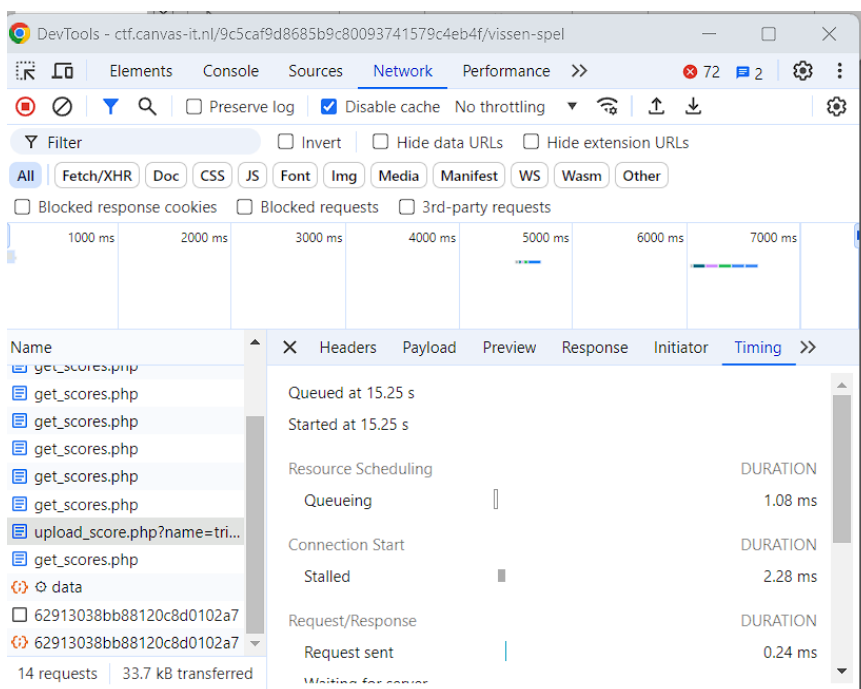
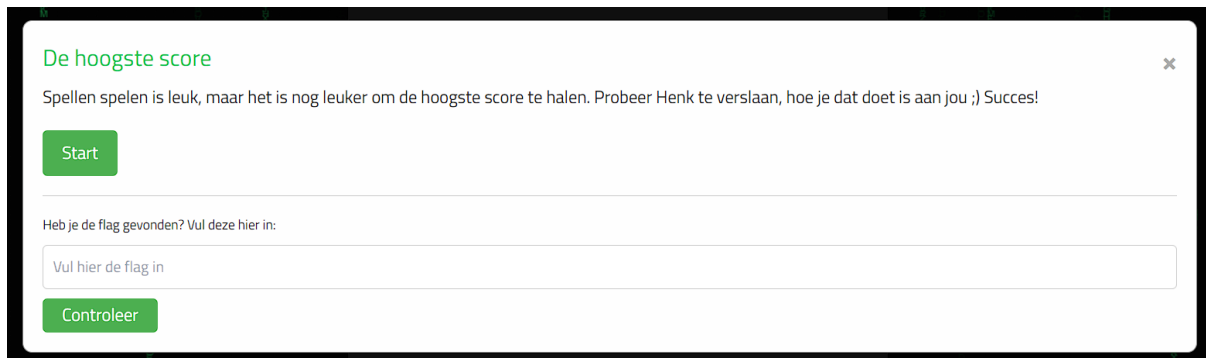


ROT13 ▼



```
Goedemiddag meneer H. Ik heb een vreemde code in mijn document van u staan:  
flag{546e4a5962457849546e46616132527561546c5a526c524e553238314c7a5a4f4d7a4e734f446  
47264455933567a5a6f596a56325a58566b637a303d}
```

Opdracht 6: Javascript aanpassen via Inspect Elements



Opdrachten

Opdracht: 1

Opdracht: 2

Opdracht: 3

Opdracht: 4

Opdracht: 5

Opdracht: 6 (Voltooid)

Speler statistieken (trieee)

Je bent al 3 minuten en 58 seconden bezig.

Je hebt 1 van de 6 opdrachten gehaald.

Aan de hand van de spelersstatistieken kan gekeken worden in hoeverre iemand de opdrachten kan oplossen.

Bijlage 7: Voorbeeld van games die worden nagebouwd


Dit is een vissengame die ook verwerkt is in de CTF Junior. Gemaakt door een jongen toen hij 14 jaar was.

Origineel:


Alle Spiele > Geleentheidsspele > Franchise: Electronic Arts > Insaniquarium Deluxe

Insaniquarium Deluxe

Communityhub



Tank 1-5



INSANIQUARIUM!

DELUXE

The craziest aquarium game ever! Tend to your fish, keep them happy and they'll reward you with coins and jewels. Buy tank upgrades or egg parts which hatch different in-tank pets. These pets can help you feed your fish, collect coins, or even protect against the aliens that will invade your tank.

KÜRZLICHE REZENSIONEN: **Außerst positiv** (102)
ALLE REZENSIONEN: **Außerst positiv** (4,947)

VERÖFFENTLICHUNG: 30. Aug. 2006

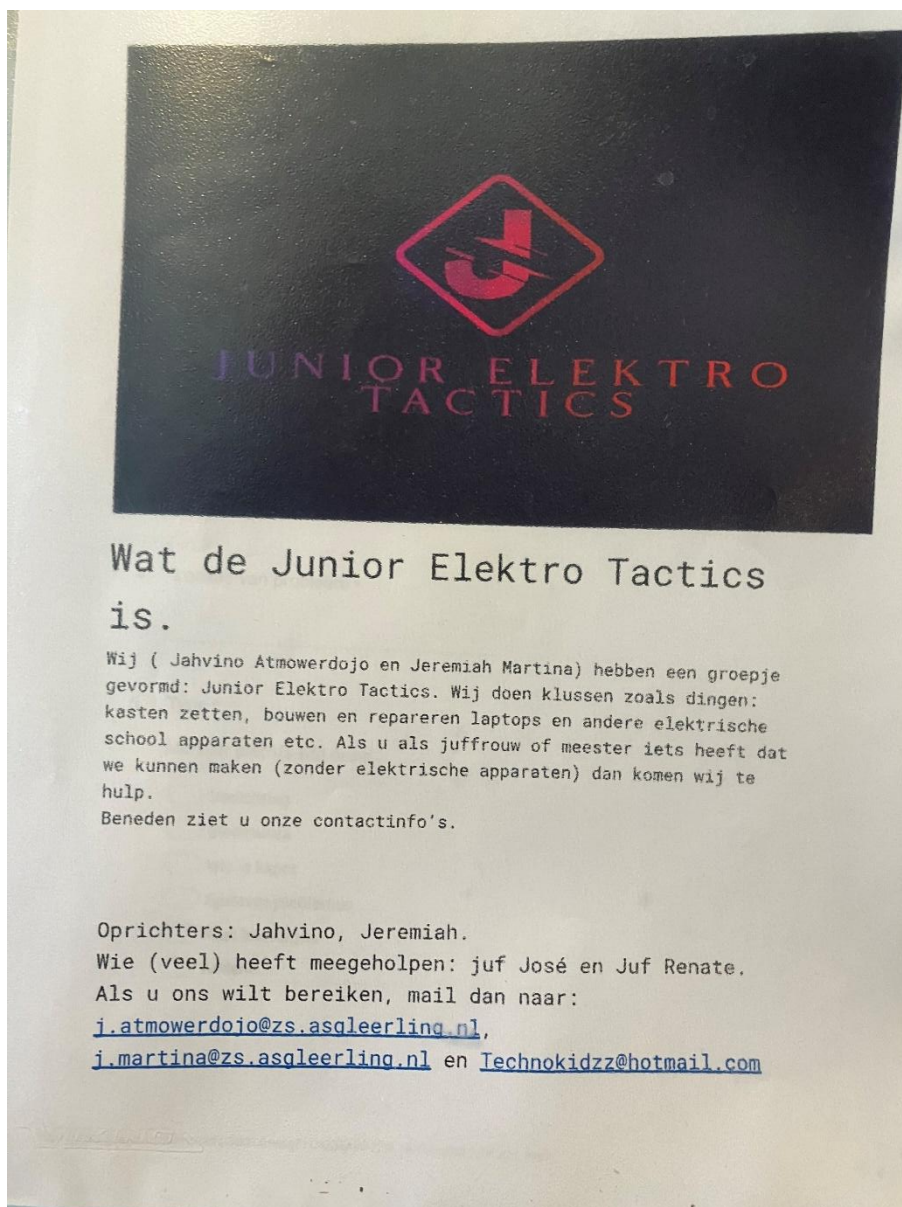
ENTWICKLER: PopCap Games, Inc.

Sind Sie damit einverstanden, dass wir optionale Cookies verwenden, um die Inhalte für Sie zu personalisieren und den Website- [Alle akzeptieren](#)

Namaak:



Bijlage 8: Flyer Junior Elektro Tactics



Bijlage 9: Handleiding met kenmerken vroegsignalering



Handleiding herkenning voor docenten versie 1



Gemeente Almere



Sneek, september 2024

Een cyberbrein: hoe herken je dat nu?

Een "jong cyberbrein" is gedefinieerd als een jongere met een uitzonderlijk talent en interesse in computers en digitale technologieën. Deze kinderen vallen op door hun vermogen om complexe taken uit te voeren met een computer, wat ver boven het niveau van hun leeftijdsgenoten ligt. Uit de theorie komen kenmerken van jonge cyberbreinen zoals:

1. **Opmerkelijke kennis en interesse in computers en digitale systemen:** Deze kinderen hebben een diepe nieuwsgierigheid naar hoe technologie werkt en het kan maar zo zijn dat ze al programmeren bijvoorbeeld.
2. **Halen graag dingen uit elkaar** om hun werking te begrijpen.
3. **Hyperfocus en probleemoplossend vermogen:** Ze kunnen zich intensief richten op problemen totdat deze zijn opgelost.
4. **Creativiteit:** Ze bedenken vaak out-of-the-box oplossingen voor problemen.
5. **Autodidactisch vermogen:** Ze leren vaak zelfstandig en ontwikkelen hun vaardigheden zonder veel externe hulp.
6. **Goede beheersing van de Engelse taal:** Omdat veel van hun tijd online wordt doorgebracht, spreken en begrijpen ze vaak goed Engels.
7. **Analytische vaardigheden:** Ze zijn goed in het analyseren en begrijpen van complexe systemen en situaties.
8. **Minder offline sociale contacten:** Ze hebben meestal meer online contacten dan offline relaties.

Ethical hackers en ouders vullen hier vaak nog deze kenmerken op aan:

9. **Eerlijk:** ze zeggen wat ze zien ongeacht de context/situatie/gesprekspartner;
10. Door een **sterk gevoel voor rechtvaardigheid** lopen ze niet zomaar mee in de maatschappelijke ordening met regels en systemen. Zeker als regels niet logisch zijn, kan dat leiden tot **dwars** gedrag;
11. **Hulpvaardig:** helpen vaak de juf of meester met allerlei ICT-vragen maar ook anderen in hun sociale context. Ook als daar niet altijd om gevraagd wordt;
12. **Eigen-wijs:** cyberbreinen hebben vaak een "andere" manier van leren is en komen soms op heel creatieve wijze tot oplossingen/antwoorden. Niet altijd volgens het boekje maar wel een goed antwoord.

Deze kenmerken maken het mogelijk om het talent van deze kinderen vroegtijdig te leren herkennen en ze daarna te kunnen begeleiden zodat ze hun talenten op een positieve manier kunnen ontwikkelen en niet het criminele pad opgaan.

Motivaties om te hacken

Uit onderzoek blijkt dat de belangrijkste positieve motivaties voor jonge cyberbreinen om te gaan hacken zijn:

1. Nieuwsgierigheid:

- Veel jonge hackers worden gedreven door een diepe nieuwsgierigheid naar hoe dingen werken in de digitale wereld. Ze willen de geheimen van technologie ontrafelen en begrijpen hoe systemen en netwerken functioneren.

2. Uitdaging en Spanning:

- De spanning en uitdaging van het hacken trekken veel jongeren aan. Het is een intellectuele puzzel die hen uitdaagt om hun technische vaardigheden en probleemoplossend vermogen te testen en te verbeteren.

3. Digitale Veiligheid:

- Een aantal jonge hackers begint met hacken vanuit een gevoel van verantwoordelijkheid voor digitale veiligheid. Ze willen kwetsbaarheden in systemen ontdekken en deze melden om de veiligheid van deze systemen te verbeteren.

4. Experimenteren en Leren:

- Jonge cyberbreinen vinden het leuk om te experimenteren met technologie. Het proces van proberen, falen en leren is voor hen zeer motiverend. Dit hands-on leren helpt hen om hun vaardigheden verder te ontwikkelen en te verfijnen.

Deze motivaties zijn sterk gekoppeld aan de behoefte van jonge cyberbreinen om te begrijpen, te creëren en bij te dragen aan een veiligere digitale omgeving.

En dan?

Denk je nu? Hee maar dan ken ik wel een mogelijk cyberbrein. Dan zouden we vanuit het project Cyberbreinen in Beeld graag kijken hoe we dit cyberbrein kunnen begeleiden om zijn talent op een goede manier te leren inzetten en te ontwikkelen. Graag kijken we naar mogelijkheden in Almere dan wel landelijk.

Je kan hiervoor altijd contact opnemen met:
Henk van Ee (Stichting Cyberbrein.nl)
Tel:06-42158182
Henk.van.ee@cyberbrein.nl

Talent gebruiken op school

Hier zijn een aantal tips om jonge cyberbreinen op een positieve manier in te zetten om de school veiliger te houden:

1. **Organiseer een Cybersecurity Club of Werkgroep:** Creëer een speciale club of werkgroep waar jonge cyberbreinen samen kunnen komen om hun kennis en vaardigheden te delen. Binnen deze groep kunnen ze werken aan projecten die de digitale veiligheid van de school verbeteren, zoals het controleren van netwerkbeveiliging of het ontwikkelen van bewustwordingscampagnes voor medeleerlingen.
2. **Stimuleer Ethical Hacking:** Bied lesmodules of workshops aan over ethical hacking. Leg uit wat ethical hacking inhoudt en waarom het belangrijk is. Laat de leerlingen onder begeleiding van een IT-expert of docent met kennis van zaken ethische hackmethoden toepassen op de schoolnetwerken om kwetsbaarheden te identificeren en op te lossen. Dit kan hun technische vaardigheden verbeteren en tegelijkertijd bijdragen aan de veiligheid van de school.
3. **Betrek ze bij Technische Ondersteuning:** Maak jonge cyberbreinen onderdeel van het IT-ondersteuningsteam van de school. Ze kunnen helpen bij het oplossen van technische problemen, het onderhouden van hardware en software, en het monitoren van het netwerk voor verdachte activiteiten. Dit geeft hun praktische ervaring en zorgt ervoor dat ze actief bijdragen aan een veilige schoolomgeving.
4. **Implementeer Cybersecurity Projecten:** Geef deze leerlingen verantwoordelijkheid over specifieke cybersecurityprojecten, zoals het ontwikkelen van een veilig wachtwoordbeleid of het opzetten van een veilige opslag voor gevoelige gegevens. Dit kan in de vorm van een schoolproject of een extra-curriculaire activiteit. Zorg ervoor dat ze regelmatig hun bevindingen en verbeteringen presenteren aan de schoolleiding en hun medeleerlingen, zodat hun werk erkend en gewaardeerd wordt.

Door deze tips te volgen, kunnen docenten niet alleen de digitale veiligheid van de school verbeteren, maar ook de talenten van jonge cyberbreinen op een positieve manier benutten en hen aanmoedigen om hun vaardigheden verder te ontwikkelen in een ethische en constructieve richting.

Talent buiten school

Deze tips kunnen ook buiten school natuurlijk. Laat jonge cyberbreinen meehelpen de digitale veiligheid van organisaties/sportclubs/gemeentes onderzoeken bijvoorbeeld.

In Den Haag zijn hier goede ervaringen mee opgedaan:
<https://www.hackthehague.com/>

Hack the Hague is een jaarlijkse ethische hackwedstrijd georganiseerd door de gemeente Den Haag in samenwerking met cybersecuritypartners. Tijdens dit evenement worden ethische hackers uitgenodigd om kwetsbaarheden in de digitale infrastructuur van de gemeente op te sporen. Het doel is om de cyberweerbaarheid van de stad te vergroten door potentiële beveiligingslekken te identificeren en op te lossen voordat kwaadwillenden hiervan misbruik kunnen maken. Deelnemers kunnen zowel individuele hackers als teams zijn, en er zijn prijzen te winnen voor de beste bevindingen. Door deze wedstrijd stimuleert de gemeente Den Haag de samenwerking tussen overheid en cybersecurity-experts om samen een veiligere digitale omgeving te creëren.

Leren en Doen

Hieronder een aantal mogelijkheden voor jonge cyberbreinen om te leren op diverse platformen.

Codecademy:

- Omschrijving: Een online leerplatform dat interactieve cursussen biedt in verschillende programmeertalen zoals Python, JavaScript, HTML, CSS en meer.
- Doel: Het toegankelijk maken van coderen en programmeren voor iedereen, van beginners tot gevorderden.

VulnHub:

- **Omschrijving:** Een platform dat gratis virtuele machines en applicaties biedt voor beveiligingstrainingen en pentesten.

- **Doel:** Het bieden van een veilige omgeving voor beveiligingsonderzoekers om hun vaardigheden in kwetsbaarheidsanalyse en ethisch hacken te verbeteren.
- **DIVD Academy:**
 - **Omschrijving:** Een onderdeel van het Dutch Institute for Vulnerability Disclosure (DIVD), gericht op het trainen van mensen in cybersecurity en kwetsbaarheidsdetectie.
 - **Doel:** Het verhogen van het kennisniveau en de vaardigheden in cybersecurity binnen Nederland door middel van trainingen en workshops.
- **Challenge the Cyber:**
 - **Omschrijving:** Een competitie gericht op jongeren om hun cybervaardigheden te testen en te verbeteren door middel van uitdagende opdrachten en scenario's.
 - **Doel:** Het identificeren en stimuleren van jong cybertalent en het vergroten van hun interesse en vaardigheden in cybersecurity.
- **Stichting Cyberbrein.nl:**
 - **Omschrijving:** Een organisatie die zich richt op het identificeren en begeleiden van jong cybertalent om hen te helpen hun vaardigheden op een positieve manier te ontwikkelen.
 - **Doel:** Het voorkomen dat jong talent afglijdt naar cybercriminaliteit door hen te ondersteunen en te begeleiden naar ethische en professionele toepassingen van hun vaardigheden.

HackShield:

- **Omschrijving:** HackShield is een educatief spel dat kinderen tussen de 8 en 12 jaar leert over cybersecurity en online veiligheid door middel van gamification. Ook in varianten die gericht zijn op Ethical Hacking;
- **Doel:** Het bewustmaken van kinderen over de gevaren van het internet en hen leren hoe ze zichzelf en anderen kunnen beschermen tegen cyberdreigingen. Het spel combineert avontuur en educatie om de interesse van jonge kinderen te wekken en hen waardevolle cybersecurity vaardigheden bij te brengen.

FreeCodeCamp:

- **Omschrijving:** FreeCodeCamp is een non-profit online platform dat gratis cursussen en certificeringen biedt in webontwikkeling en programmeren. De cursussen omvatten onderwerpen zoals HTML, CSS, JavaScript, Python, en meer.
- **Doel:** Het toegankelijk maken van programmeer- en webontwikkelingsonderwijs voor iedereen, ongeacht hun achtergrond of financiële situatie. Het platform biedt ook hands-on projecten en een gemeenschap van lerenden om samen te werken en elkaar te ondersteunen.

Bijlage 10: Profiel in de praktijk en comment teamcaptain Challenge The Cyber

Let op: hier is niet het volledige profiel van alle kenmerken voorgelegd maar is een tussentijdse samenvatting gebruikt van een aantal kenmerken.

Een cyberbrein: hoe herken je dat nu?

Een "jong cyberbrein" is gedefinieerd als een jongere met een uitzonderlijk talent en interesse in computers en digitale technologieën. Deze kinderen vallen op door hun vermogen om complexe taken uit te voeren met een computer, wat ver boven het niveau van hun leeftijdsgenoten ligt. Uit de theorie komen kenmerken van jonge cyberbreinen zoals:

1. **Opmerkelijke kennis en interesse in computers en digitale systemen:** Deze kinderen hebben een diepe nieuwsgierigheid naar hoe technologie werkt en het kan maar zo zijn dat ze al programmeren bijvoorbeeld.
2. **Halen graag dingen uit elkaar om hun werking te begrijpen.**
3. **Hyperfocus en probleemoplossend vermogen:** Ze kunnen zich intensief richten op problemen totdat deze zijn opgelost.
4. **Creativiteit:** Ze bedenken vaak out-of-the-box oplossingen voor problemen.
5. **Autodidactisch vermogen:** Ze leren vaak zelfstandig en ontwikkelen hun vaardigheden zonder veel externe hulp.
6. **Goede beheersing van de Engelse taal:** Omdat veel van hun tijd online wordt doorgebracht, spreken en begrijpen ze vaak goed Engels.
7. **Analytische vaardigheden:** Ze zijn goed in het analyseren en begrijpen van complexe systemen en situaties.
8. **Minder offline sociale contacten:** Ze hebben meestal meer online contacten dan offline relaties.

Ethical hackers en ouders vullen hier vaak nog deze kenmerken op aan:

9. **Eerlijk:** ze zeggen wat ze zien ongeacht de context/situatie/gesprekspartner;
10. Door een **sterk gevoel voor rechtvaardigheid** lopen ze niet zomaar mee in de maatschappelijke ordening met regels en systemen. Zeker als regels niet logisch zijn, kan dat leiden tot **dwars** gedrag;
11. **Hulpvaardig:** helpen vaak de juf of meester met allerlei ICT-vragen maar ook anderen in hun sociale context. Ook als daar niet altijd om gevraagd wordt;
12. **Eigen-wijs:** cyberbreinen hebben vaak een "andere" manier van leren is en komen soms op heel creatieve wijze tot oplossingen/antwoorden. Niet altijd volgens het boekje maar wel een goed antwoord.

Deze kenmerken maken het mogelijk om het talent van deze kinderen vroegtijdig te leren herkennen en ze daarna te kunnen begeleiden zodat ze hun

Ik lees net de PDF in de mail van Stichting Cyberbrein ik moet even zeggen dat ik mij inderdaad heel goed kan herkennen in al deze 12 punten 😂😂😂
Erg mooi om te zien dat ze heel accuraat dit hebben weten te verwoorden, mooie missie

Bijlage 11: Online ronselen via Discord

Dit is een screenshot uit de Discordserver van de re_B00TCMP die door de Stichting Cyberbrein.nl beheerd wordt.

